

思科 Firepower 4100/9300 FXOS 发行说明， 2.4(1)

首次发布日期: 2018 年 10 月 25 日

上次修改日期: 2019 年 9 月 30 日

思科 Firepower 4100/9300 FXOS 发行说明， 2.4(1)

本文档包含思科 Firepower 可扩展操作系统 (FXOS) 2.4(1) 的版本信息。

此版本说明可作为文档规划图中所列出的其他文档的补充内容：

- <http://www.cisco.com/go/firepower9300-docs>
- <http://www.cisco.com/go/firepower4100-docs>



注释 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 上的文档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。

简介

思科 Firepower 安全设备是网络和内容安全解决方案的下一代平台。Firepower 安全设备是思科以应用为中心的基础设施 (ACI) 安全解决方案的一部分，并且提供为实现可扩展性、一致控制和简化管理而构建的灵活、开放、安全的平台。

Firepower 安全设备提供以下功能：

- 基于机箱的模块化安全系统 - 提供高性能、灵活的输入/输出配置和可扩展性。
- Firepower 机箱管理器 - 图形用户界面可简单、直观地显示当前机箱状态并支持简化的机箱功能配置。
- FXOS CLI - 提供基于命令的接口，用于配置功能，监控机箱状态和访问高级故障排除功能。
- FXOS REST API - 允许用户以编程方式配置和管理其机箱。

最新产品

FXOS 2.4.1.249 的新增功能

除了早期版本中包含的功能以外，思科 FXOS 2.4.1.249 还推出了以下新功能：

- 各种问题的修复补丁（请参阅 [FXOS 2.4.1.249 中已解决的漏洞](#)，第 9 页）。

FXOS 2.4.1.244 的新增功能

除了早期版本中包含的功能以外，思科 FXOS 2.4.1.244 还推出了以下新功能：

- 各种问题的修复补丁（请参阅 [FXOS 2.4.1.244 中已解决的漏洞](#)，第 9 页）。

FXOS 2.4.1.238 的新增功能

除了早期版本中包含的功能以外，思科 FXOS 2.4.1.238 还推出了以下新功能：

- 解决各种问题（请参阅 [FXOS 2.4.1.238 中已解决的漏洞](#)）。

FXOS 2.4.1.234 的新增功能

除了早期版本中包含的功能以外，思科 FXOS 2.4.1.234 还推出了以下新功能：

- 解决各种问题（请参阅 [FXOS 2.4.1.234 中已解决的漏洞](#)）。

FXOS 2.4.1.222 的新增功能

除了早期版本中包含的功能以外，思科 FXOS 2.4.1.222 还推出了以下新功能：

- 解决各种问题（请参阅 [FXOS 2.4.1.222 中已解决的漏洞](#)）。

FXOS 2.4.1.214 的新增功能

除了早期版本中包含的功能以外，思科 FXOS 2.4.1.214 还推出了以下新功能：

- 支持 Firepower 威胁防御版本 6.3。
- Firepower 威胁防御的多实例功能（请参阅 [Firepower 威胁防御的多实例功能](#)）。



注释 需要 Firepower 威胁防御版本 6.3 或更高版本。

- 解决各种问题（请参阅 [FXOS 2.4.1.214 中已解决的漏洞](#)）。

FXOS 2.4.1.101 的新增功能

思科 FXOS 2.4.1.101 推出了以下新功能：

- 支持 ASA 9.10(1)。
- 支持 ASA 逻辑设备的透明模式部署。

您现在可以在部署 ASA 时指定透明模式或路由模式。

新增/修改的 FXOS 命令：**enter bootstrap-key FIREWALL_MODE**、**set value routed**、**set value transparent**

新增/修改的 Firepower 机箱管理器菜单项：

逻辑设备 > 添加设备 > 设置

新增/修改的选项：**Firewall 模式**下拉列表

- 集群控制链路可自定义 IP 地址。

默认情况下，群集控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署群集时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的群集控制链路接口 IP 地址：

127.2.chassis_id.slot_id。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的群集控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。

新增/修改的命令：**set cluster-control-link network**

新增/修改的屏幕：

逻辑设备 > 添加设备 > 集群信息

新增/修改的选项：**CCL 子网 IP 字段**



注释 ASA 9.9.2 及更高版本和 Firepower 威胁防御 6.3.0 及更高版本支持与 **CCL 子网 IP 字段** 选项配合使用

- 在开启模式下支持数据 Etherchannel。

现在可以将数据和数据共享 Etherchannel 设置为“主用” LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。

新增/修改的菜单项：

接口 > 所有接口 > 编辑端口通道 > 模式

新增/修改的命令：**set port-channel-mode**

- 现在，您可以在 Firepower 4110 设备上启用具有 ASA 的 Radware DefensePro (vDP)。
- 在机箱间集群场景中，可在独立配置下部署 Radware DefensePro (vDP) 应用程序。
- 现在，您可以选择不将主机名数据发送到 Firepower 4100 系列设备上的思科智能许可。
- 现在，您可以一次确认多个故障。
- Firepower 机箱管理器现在显示上传图像时的上传百分比。

- 解决各种问题（请参阅 [FXOS 2.4.1.101 中已解决的漏洞](#)）。

Firepower 威胁防御的多实例功能



注释 需要 FTD 版本 6.3 或更高版本。

您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 Firepower 威胁防御容器实例。以前，您仅可部署单个本地应用实例。此外，仍支持本地实例。对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。

要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。部署容器实例时，必须指定分配的 CPU 核心数量；系统会根据核心数量动态分配 RAM。此资源管理允许您自定义每个实例的性能。

您可以在 2 个独立机箱上使用容器实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱各 10 个实例，您可以创建 10 个高可用性对。不支持群集。



注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全 Firepower 威胁防御功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。Firepower 威胁防御不支持多情景模式。

参阅下文以了解每个型号的最大容器实例数：

- Firepower 4110-3
- Firepower 4120-3
- Firepower 4140-7
- Firepower 4150-7
- Firepower 9300 SM-24 安全模块-7
- Firepower 9300 SM-36 安全模块-11
- Firepower 9300 SM-44 安全模块-14

新增/修改的 Firepower 机箱管理器菜单项：

概述 > 设备

接口 > 所有接口 > 新增下拉菜单 > 子接口

接口 > 所有接口 > 类型

逻辑设备 > 添加设备

平台设置 > Mac 池

平台设置 > 资源配置文件

新增/修改的 FXOS 命令：

connect ftd name、connect module telnet、create bootstrap-key PERMIT_EXPERT_MODE、create resource-profile、create subinterface、scope auto-macpool、set cpu-core-count、set deploy-type、set port-type data-sharing、set prefix、set resource-profile-name、set vlan、scope app-instance ftd name、show cgroups container、show interface、show mac-address、show subinterface、show tech-support module app-instance、show version

新增/修改的 Firepower 管理中心菜单项：

设备 > 设备管理 > 编辑图标 > 接口选项卡

适用于 ASA 应用程序的 FXOS CLI 更改

处理 ASA 逻辑设备时使用的 FXOS CLI 命令已修改。

新增/修改的 FXOS 命令：

connect asa name、create app-instance asa name、scope app-instance asa name、show app-instance asa name

软件下载

可从以下某个 URL 下载 FXOS 的软件映像及受支持的应用：

- Firepower 9300 - <https://software.cisco.com/download/type.html?mdfid=286287252>
- Firepower 4100 - <https://software.cisco.com/download/navigator.html?mdfid=286305164>

有关特定版本 FXOS 支持的应用的信息，请参阅以下 URL 中的思科 FXOS 兼容性指南：

<http://www.cisco.com/c/en/us/td/docs/security/Firepower/fxos/compatibility/fxos-compatibility.html>

重要说明

- 如果您使用硬件旁路功能，则必须升级到 FXOS 2.4.1.238。在 2.4.1.238 之前的 FXOS 版本中，端口可能会在不发生故障事件的情况下进入旁路状态。如果发生这种情况，您必须使用 Firepower 管理中心使端口恢复到备用模式。
- 在 FXOS 2.4(1) 中，如果您在 FIPS 模式下使用 IPSec 安全通道，则 IPSec 对等体必须支持 RFC 7427。
- 如果在升级到 FXOS 2.4(1) 后重新初始化安全模块，则当稍后降级到较早的 FXOS 版本时，您可能会收到有关该安全模块上的磁盘分区不兼容的错误消息。要解决此问题，您需要在降级后重新初始化安全模块。
- 在 Firepower 4110 或 4120 设备上当前运行的 Firepower 威胁防护应用程序的服务链中配置 Radware DefensePro (vDP) 时，安装将会失败并显示故障警报。解决办法是在安装 Radware DefensePro 应用程序之前停止 Firepower 威胁防护应用程序实例。请注意，此问题和解决方法适用于 Firepower 4110 和 4120 设备上使用 Firepower 威胁防御链接的所有受支持版本的 Radware DefensePro 服务。

- 固件升级 - 建议使用最新固件升级 Firepower 4100/9300 安全设备。有关如何安装固件更新和每个更新中包含的修补程序的信息，请参阅 <https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/firmware-upgrade/fxos-firmware-upgrade.html>。
- 升级网络或安全模块时，系统会生成某些故障，然后自动清除。其中包括“不支持 热插拔”或者“在联机状态时删除模块”错误。如《思科 Firepower 9300 硬件安装指南》或《思科 Firepower 4100 系列硬件安装指南》中所述，如果您按照适当的步骤操作，这些故障将自动清除，无需执行其他操作。

适配器引导加载程序升级

FXOS 2.4(1) 包含额外的测试，用于验证安全设备上的安全模块适配器。安装 FXOS 2.4.1.101 或更高版本后，您可能会收到一则类似以下内容的严重故障，指示您应更新安全模块适配器的固件：

严重故障 *F1715 2017-05-11T11:43:33.121 339561* 安全模块 1 上的适配器 1 需要进行重要的固件升级。请参阅随本版本发布的 FXOS 发行说明中的适配器引导程序升级说明。

如果收到上述消息，请按以下程序为适配器更新启动映像：

1. 连接到 Firepower 安全设备上的 FXOS CLI。有关说明，请参阅《思科 Firepower 4100/9300 FXOS CLI 配置指南 [2.4(1)]》或《思科 Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南 [2.4(1)]》中的“访问 FXOS CLI”主题。

2. 输入您要更新其启动镜像的适配器的适配器模式：

```
fxos-chassis# scope adapter 1/security_module_number/adapter_number
```

3. 输入 **show image** 以查看可用的适配器映像，并验证是否可以安装
fxos-m83-8p40-cruzboot.4.0.1.62.bin:

```
fxos-chassis /chassis/server/adapter # show image
Name Type Version
-----
```

```
fxos-m83-8p40-cruzboot.4.0.1.62.bin Adapter Boot 4.0(1.62)
```

```
fxos-m83-8p40-vic.4.0.1.51.gbin Adapter 4.0(1.51)
```

4. 输入 **update boot-loader** 将适配器启动映像更新到版本 4.0.1.62:

```
fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause
adapter to become UNUSABLE!
After upgrade has completed, blade will be power cycled automatically
fxos-chassis /chassis/server/adapter* # commit-buffer
```

5. 输入 **show boot-update status** 以监控更新状态:

```
fxos-chassis /chassis/server/adapter # show boot-update status
State: Updating
fxos-chassis /chassis/server/adapter # show boot-update status
State: Ready
```

6. 输入 **show version detail** 以验证更新是否成功:



注释

您的 **show version detail** 输出可能不同于以下示例。不过，请验证并确保 Bootloader-Update-Status 为“就绪”且 Bootloader-Vers 为 4.0(1.62)。

```
fxos-chassis /chassis/server/adapter # show version detail
Adapter 1:
Running-Vers: 5.2(1.2)
Package-Vers: 2.2(2.17)
Update-Status: Ready
Activate-Status: Ready
Bootloader-Update-Status: Ready
Startup-Vers: 5.2(1.2)
Backup-Vers: 5.0(1.2)
Bootloader-Vers: 4.0(1.62)
```

系统要求

您可以使用以下浏览器访问 Firepower 机箱管理器：

- Mozilla Firefox - 版本 42 及更高版本
- Google Chrome - 版本 47 及更高版本
- Microsoft Internet Explorer - 版本 11 及更高版本

我们使用 Mozilla Firefox 版本 42、Google Chrome 版本 47 和 Internet Explorer 版本 11 对 FXOS 2.4(1) 进行了测试。这些浏览器的其他版本预计会正常运行。但是，如果您遇到任何浏览器相关问题，我们建议您恢复到其中一个经过测试的版本。

升级说明

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备当前运行的是 FXOS 2.0(1) 或更高的内部版本，可以将其升级到 FXOS 2.4(1.214)。

有关升级说明，请参阅《[思科 Firepower 4100/9300 升级指南](#)》。

安装说明

- 升级到 FXOS 2.4(1) 最高可能需要 45 分钟。请相应规划您的升级活动。
- 如果要升级运行独立逻辑设备的 Firepower 9300 或 Firepower 4100 系列安全设备，或者要升级运行机箱内群集的 Firepower 9300 安全设备，则升级期间流量不会通过该设备。
- 如果要升级属于某机箱间群集的 Firepower 9300 或 Firepower 4100 系列安全设备，则升级期间流量不会通过正在升级的设备。但是，该群集中的其他设备仍然会通过流量。
- 官方不支持 FXOS 映像降级。思科唯一支持的 FXOS 映像版本降级方法是对设备执行完整的重新映像。

尚未解决和已解决的漏洞

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。



注释 您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果您还没有此帐户，请[注册一个帐户](#)。

有关思科漏洞搜索工具的详细信息，请参阅[漏洞搜索工具帮助及常见问题](#)。

遗留漏洞

下表列出了在发布此发行说明时尚未解决的漏洞。

表 1: 影响 **FXOS 2.4(1)** 的遗留漏洞

标识符	描述
CSCuw31077	应验证应用于接口的过滤器
CSCux63101	内存阵列下的所有内存在“可操作”列中显示为“未知”
CSCux77947	当以高速率发送数据时，Pcap 文件大小未正确更新
CSCux98517	应允许从机箱管理器取消修饰 VDP 的数据端口
CSCuz93180	如果验证失败，AAA LDAP 配置不会保留信息
CSCvc03494	无法将 Radware vDP 添加到 APSolute Vision 中。解决方法是，必须手动下载设备驱动程序并将其安装到 Vision 中。
CSCvc44522	警告：管理控制器服务器 1/1 中的日志容量处于非常低的警告状态
CSCvd90177	在运行 FXOS 2.2.1.57 的 QP-D 上执行 MIO 重新加载后，刀片进入故障状态
CSCvj96380	如果开关旁路使能失败，SAM 耦合器应强制 FTW 旁路
CSCvk46399	MIO 重新启动后看到 svc_sam_bladeAG_log 核心
CSCvk61563	在 KP ASA 上，重新引导后不创建 /root/.ssh
CSCvm66013	MIO 在重新引导过程中挂起。发现内核恐慌问题。
CSCvm84592	当为捕获会话完成“编辑会话”时，过滤器配置丢失
CSCvo64240	无法确认“未关联服务配置文件 ssp-sprof”警告警报。
CSCvo68997	FXOS ip-block 无法恢复 sam.configure

FXOS 2.4.1.249 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞，这些漏洞在 FXOS 2.4.1.249 中已得到解决：

表 2: FXOS 2.4.1.249 中已解决的漏洞

标识符	描述
CSCvh68895	FPR9300 上显示额外的“本地磁盘 3”
CSCvk70849	如果密码超过 32 个字符，则 FCMGUI 身份验证失败，并出现“无法登录。身份验证失败”
CSCvm76266	线程名称 cli_xml_server 发生 Lina 回溯
CSCvm87556	升级 92.5(1.232) 时，固件自动安装状态失败
CSCvm96265	启用了禁用 HTTP 选项
CSCvn24594	在启动 NTPD 之前，从管理引擎添加刀片系统时钟的 NTPDATE 更新
CSCvn45138	从机箱管理器 UI 进行引导程序更改后，FTD 被取消注册
CSCvo40340	FPR4100: 在风扇 OIR 后，序列号、型号和供应商为黑色
CSCvo79145	从 k9.2.4.1.222.SPA 升级 k9.2.6.1.118.SPA 时，FTD 不启动（磁盘配额问题）
CSCvp35769	[ciam] Apache HTTP 服务器 URL 规范化拒绝服务漏洞
CSCvq17910	在应用重新引导或集群重新加入时，不在机箱上编程多播 MAC
CSCvq19641	评估 TCP_SACK 的 Firepower 4k/9k 管理引擎
CSCvq33916	使用 40gb bidi 至 40/100 bidi 时，FP 4100 和交换机之间链路断开

FXOS 2.4.1.244 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞，这些漏洞在 FXOS 2.4.1.244 中已得到解决：

表 3: FXOS 2.4.1.244 中已解决的漏洞

标识符	描述
CSCvn77125	FXOS: copy 命令应允许使用通配符以传输多个文件
CSCvo85861	传播链路状态未显示在 FTD CLI 中
CSCvo90987	针对客户设备上的 bcm_usd.log 文件的调试链路关闭/摆动问题进行了增强
CSCvp10674	在安装 vDP 并将 FXOS 升级到版本 2.4.1 后，FTD 无法联机

标识符	描述
CSCvp15176	安装在 Firepower 设备上安装的应用可能会报告通信故障并将自己作为主用/主应用。
CSCvp21561	由于内核修补程序与 Cruz 内核版本不兼容，Cruz 适配器崩溃
CSCvp40260	防止将 STP 和 FC 帧发送到 SUP CPU
CSCvp56801	当 4100 上仅有 1x 实例时，“show tech-support module 1 app-instance <应用名称> <标识符>”
CSCvp83437	使用本地帐户的串行控制台登录成功，但立即返回到登录提示

FXOS 2.4.1.238 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞，这些漏洞在 FXOS 2.4.1.238 中已得到解决：

表 4: FXOS 2.4.1.238 中已解决的漏洞

标识符	描述
CSCvk47441	FXOS 4100/9300: icmp 重定向永久陷入 FXOS OOB 管理路由表中
CSCvk60985	记录了计算机检查事件。可能存在硬件问题。FXOS 刀片: mcelog 支持
CSCvm72541	如果端口通道的状态为“关闭”，则 interfaceMapping 消息中的速度为 0
CSCvn46577	与 FXOS 的某些 SSH 会话不会因绝对/会话超时而超时
CSCvn98401	/Opt/cisco/platform/logs/corruptConfigs 中的许多 0 字节文件导致 LACP 问题和不稳定
CSCvo29067	FXOS 升级挂起并已开始生成 DME 核心文件
CSCvo31071	当设备重新加入群集时，流量下降。
CSCvo56910	分配给上下文的 ASA 子接口将在故障切换后间歇性停止响应
CSCvo58998	FXOS Cruz 适配器未验证逻辑设备发送的数据，导致卸载的数据包丢失
CSCvo64091	SSP: 群集从属 FTD 调配失败，因为“必要的外部端口不可用”
CSCvo75349	由于内存损坏，FXOS Blade CRUZ FW 核心转储
CSCvo87116	MTS 消息卡在 AppAG recv_q 中
CSCvp09791	FXOS/FTD 多实例部署多播流量中断

FXOS 2.4.1.234 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞，这些漏洞在 FXOS 2.4.1.234 中已得到解决：

表 5: FXOS 2.4.1.234 中已解决的漏洞

标识符	描述
CSCvn31390	计算处理器 PortSmash 侧通道信息披露漏洞
CSCvn42582	在重新引导后, FXOS “导出触发提醒” 从禁用更改为启用
CSCvn48162	NTP 通信错误可能会导致 iptables 中出现重复的条目, 从而引起 HB 错误
CSCvn56156	由于分类器表条目损坏, FXOS 平台上可能会出现无提示的数据包丢弃
CSCvn77641	无法恢复 SSP 自动旁路端口
CSCvn78014	正常关闭在数据端口上不起作用。
CSCvn90677	在 FTD 安装过程中, 设置磁盘分区大小可能会失败, 而不给出提示
CSCvn90701	FTD 安装期间发生的错误不会被记录
CSCvn93793	发生 SSD 故障时, 不进行故障切换
CSCvo10712	当 cspCfgXml 损坏时, SMA 每分钟创建一个新文件
CSCvo28623	ssp_admin_status.sh 在升级失败后检测到遗留的元数据 json 文件
CSCvo28634	MIO 对应用实例报告错误的状态
CSCvo30356	升级后端口通道处于挂起状态
CSCvo44029	当 FTD 仍正常运行时, 自动旁路端口对进入旁路状态

FXOS 2.4.1.222 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞, 这些漏洞在 FXOS 2.4.1.222 中已得到解决:

表 6: FXOS 2.4.1.222 中已解决的漏洞

标识符	描述
CSCvm53282	FTD: 通过 ICMP 重定向添加的路由表永远陷入路由表缓存中
CSCvn23221	Cruz ASIC 因 ecpumgr 断言恐慌而崩溃
CSCvn36413	特定版本格式/命名的升级-恢复极端情况案例

FXOS 2.4.1.214 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞, 这些漏洞在 FXOS 2.4.1.214 中已得到解决:

表 7: FXOS 2.4.1.214 中已解决的漏洞

标识符	描述
CSCvg72548	Maverick 前面板和背板数据包捕获中观察到双 VLAN 信头
CSCvj06276	FXOS: 无法通过 snmpwalk 检索正确的磁盘使用值 (/dev/sdaX)
CSCvk09976	将相同的过滤器同时应用于同一接口的物理端口和应用端口时, 不会捕获数据包
CSCvm21278	评估 CVE-2018-5391 (FragmentSmack) 的 ssp
CSCvm33545	系统中的时钟偏差导致 ndmain 报告服务关闭状态
CSCvm73853	在 FXOS 2.2.2.26 中运行的许可证管理器上重新加载 Firepower 机箱
CSCvn02840	从 2.2.2 升级到 2.4.1 时, sdExternalPortLink 的端口类型未知
CSCvn08869	FCM: 映像版本获取在“逻辑设备”页面中挂起
CSCvn11768	如果应用程序实例引用应用程序 CSP, 则不应将其删除
CSCvn17585	FXOS: 由于 dcosAG 崩溃, 导致意外重新加载

FXOS 2.4.1.101 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞, 这些漏洞在 FXOS 2.4.1.101 中已得到解决:

表 8: FXOS 2.4.1.101 中已解决的漏洞

标识符	描述
CSCuy21573	机箱管理器: 在更新页面中的排序被打乱
CSCvf70180	FCM 会将 DNS 搜索域列表发送到 ASDM, 而不只是一个域
CSCvg57022	机箱管理器: 登录详细信息中的时区不正确
CSCvg57037	机箱管理器: 密码“设置: 是”或否出现不正确的位置(日语)
CSCvg62443	机箱管理器 UI (“逻辑设备”页面) 不显示 FTD 设备的正确 IP
CSCvg67730	限制刀片核心文件数, 避免由于磁盘空间不足而导致不完整的刀片技术支持
CSCvg71168	即使在安全模块发生故障时也会启动 asa
CSCvg72559	启用 IPv6 过滤器数据包捕获失败

相关文档

有关 Firepower 9300 或 4100 系列安全设备及 FXOS 的更多信息, 请参阅[思科 FXOS 导航文档](#)。

网上资源

思科提供在线资源来下载文档/软件/工具、查询错误以及创建服务请求。这些资源可用于安装和配置 Firepower 软件以及解决和消除技术问题。

- 思科技术支持及下载站点: <https://www.cisco.com/c/en/us/support/index.html>
- 思科漏洞搜索工具: <https://tools.cisco.com/bugsearch/>
- 思科通知服务: <https://www.cisco.com/cisco/support/notifications.html>

使用思科技术支持及下载站点上的大多数工具时, 需要 Cisco.com 用户 ID 和密码。

联系思科

如果上面列出的联机资源无法解决您的问题, 请联系思科 TAC:

- 向思科 TAC 发送电子邮件: tac@cisco.com
- 致电思科 TAC (北美): 1.408.526.7209 或 1.800.553.2447
- 致电思科 TAC (全球): [思科全球支持联系人](#)

通信、服务和其他信息

- 要及时从思科收到相关信息, 请注册[思科配置文件管理器](#)。
- 要使用重要技术实现您期望实现的业务影响, 请访问[思科服务](#)。
- 要提交服务请求, 请访问[思科支持](#)。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务, 请访问[思科 Marketplace](#)。
- 要获取一般网络、培训和认证主题相关的信息, 请访问[思科出版社](#)。
- 要查找有关特定产品或产品系列的保修信息, 请访问[思科保修服务查找工具](#)。

