



安全模块/引擎管理

- [关于 FXOS 安全模块/安全引擎，第 1 页](#)
- [停用安全模块，第 3 页](#)
- [确认安全模块/引擎，第 3 页](#)
- [重启安全模块/引擎，第 4 页](#)
- [重新初始化安全模块/引擎，第 4 页](#)
- [确认网络模块，第 5 页](#)
- [使网络模块离线或在线，第 5 页](#)
- [刀片运行状况监控，第 7 页](#)

关于 FXOS 安全模块/安全引擎

在机箱管理器的“安全模块/安全引擎”页面上，您可以查看安全模块/引擎的状态，并在安全模块/引擎上执行各种功能：

安全模块/安全引擎 (Security Modules/Security Engine) 页面提供以下信息：

- 硬件状态 - 显示安全模块/引擎硬件的状态。
 - 开启 - 安全模块/引擎已成功启动，并且未显示任何硬件故障，即使安全模块/引擎没有与之关联的逻辑设备。
 - 正在启动 - 安全模块/引擎正在启动过程中。
 - 重启 - 安全模块/引擎正在重启过程中。
 - 关闭 - 安全模块/引擎的电源未打开或硬件故障阻止安全模块/引擎成功启动。
 - 不匹配 (Mismatch) - 安全模块已停用或插槽中安装了新的安全模块。使用“确认” (Acknowledge) 功能，使安全模块恢复正常运行状态。
 - 空 - 该插槽中未安装安全模块。
- 服务状态 - 显示安全模块/引擎上软件的状态：

- 不可用 (Not-available) - 安全模块已从插槽中移除。重新安装安全模块，使之回到正常运行状态。
- 在线 - 安全模块/引擎已安装并处于正常运行模式。
- 未响应 - 安全模块/引擎未响应。
- 令牌不匹配 (Token Mismatch) - 表示已安装到机箱插槽中的安全模块不是之前配置的安全模块。这也可能是软件安装错误引起的。使用“重新初始化(Reinitialize)”功能使安全模块恢复正常运行状态。
- 故障 - 安全模块/引擎处于故障状态。查看系统故障列表，了解有关故障状态可能原因的详细信息。您也可以将鼠标悬停在故障对应的信息图标上，以查看更多信息。

安全模块故障

- 故障保护模式 - 安全模块处于故障保护模式。在此模式下，系统会阻止启动应用。要进行故障排除或禁用故障保护模式，请连接到安全模块。也可以删除应用实例。
- HDD 错误 - 安全模块磁盘驱动器出现错误。请确认安全模块有磁盘驱动器，并且如果故障未清除，则更换故障磁盘驱动器。
- 文件系统错误 - 安全模块上的磁盘分区不兼容。重启安全模块有可能会使其从故障中恢复。如果此故障仍然存在，请将数据备份到外部设备，然后对插槽进行重新初始化。
- 格式故障 - 安全模块磁盘驱动器上的自动格式功能出现故障。重新初始化安全模块以便重新格式化。
- 电源 - 显示安全模块/引擎的电源状态：
 - 开 (On) - 使用“电源关/开 (Power off/on)”功能切换安全模块/引擎的电源状态。
 - 关 (Off) - 使用“电源关/开 (Power off/on)”功能切换安全模块/引擎的电源状态。
- 应用 - 显示安全模块/引擎上安装的逻辑设备类型。

在机箱管理器的“安全模块/安全引擎”页面上，您可以在安全模块/引擎上执行以下功能：

- 停用（仅限安全模块）- 停用安全模块后，安全模块将进入维护模式。您还可以先停用然后确认安全模块，从而纠正某些故障状态。请参阅[停用安全模块，第 3 页](#)。
- 确认 (Acknowledge) - 让新安装的安全模块上线。请参阅[确认安全模块/引擎，第 3 页](#)。
- 重启 - 重新启动安全模块/引擎。请参阅[重启安全模块/引擎，第 4 页](#)。
- 重新初始化 - 重新格式化安全模块/引擎硬盘，从安全模块/引擎上删除所有部署的应用和配置，然后重新启动系统。在重新初始化完成后，如果为安全模块/引擎配置了逻辑设备，FXOS将重新安装应用软件，重新部署逻辑设备，并自动启动应用。请参阅[重新初始化安全模块/引擎，第 4 页](#)。



警告 在重新初始化期间，安全模块/引擎上的所有应用数据都将被删除。请在重新初始化安全模块/引擎之前备份所有应用数据。

- 电源关/开 - 切换安全模块/引擎的电源状态。请参阅 [重启安全模块/引擎](#)，第 4 页。

停用安全模块

当您停用安全模块时，安全模块对象将从配置中删除，安全模块将变为非托管状态。安全模块上运行的任何逻辑设备或软件都将变为非活动状态。

如果要暂时停止使用安全模块，您可以停用安全模块。

过程

- 步骤 1** 选择安全模块 (**Security Modules**) 打开“安全模块 (Security Modules)”页面。
- 步骤 2** 要停用安全模块，点击该安全模块所对应的下线 (**Decommission**)。
- 步骤 3** 点击是 (**Yes**) 确认要停用指定的安全模块。

确认安全模块/引擎

将新的安全模块安装到机箱时，或将现有模块替换为一个具有不同产品 ID (PID) 的模块时，必须确认安全模块，然后才能开始使用该模块。

如果安全模块显示“不匹配”或“令牌不匹配”状态，这表示安装在插槽中的安全模块上的数据与之前安装在该插槽中的模块不匹配。如果安全模块上已有数据并且您确定要在新的插槽中使用它（换句话说，安全模块并非无意中安装到错误插槽），您必须重新初始化该安全模块，然后才可以向它部署逻辑设备。

过程

- 步骤 1** 选择安全模块/安全引擎 (**Security Modules/Security Engine**) 打开“安全模块/安全引擎 (Security Modules/Security Engine)”页面。
- 步骤 2** 点击您想要确认的安全模块/引擎所对应的确认 (**Acknowledge**)。
- 步骤 3** 点击是 (**Yes**) 确定您要确认指定的安全模块/引擎。

重启安全模块/引擎

按照以下步骤重启安全模块/引擎。

过程

步骤 1 选择安全模块/安全引擎 (Security Modules/Security Engine) 打开“安全模块/安全引擎 (Security Modules/Security Engine)”页面。

步骤 2 点击您想要重新引导的安全模块/引擎所对应的**重启 (Power Cycle)**。

步骤 3 执行以下操作之一：

- 点击**安全重启 (Safe Power Cycle)** 让系统等待最多五分钟，以便在系统重启指定的安全模块/引擎之前关闭安全模块/引擎上运行的应用程序。
 - 点击**立即重启 (Power Cycle Immediately)** 让系统立即重启指定的安全模块/引擎。
-

重新初始化安全模块/引擎

当安全模块/引擎重新初始化时，安全模块/引擎的硬盘将会格式化，所有安装的应用实例、配置和数据均会删除。在重新初始化完成后，如果为安全模块/引擎配置了逻辑设备，FXOS 将重新安装应用软件，重新部署逻辑设备，并自动启动应用。



注意 在重新初始化期间，安全模块/引擎上的所有应用数据都将被删除。请在重新初始化安全模块/引擎之前备份所有应用数据。

过程

步骤 1 选择安全模块/安全引擎 (Security Modules/Security Engine) 打开“安全模块/安全引擎” (Security Modules/Security Engine) 页面。

步骤 2 点击您想要重新初始化的安全模块/引擎所对应的**重新初始化**。

步骤 3 点击是确认您要重新初始化指定的安全模块/引擎。

安全模块/引擎会重启，安全模块上的所有数据均会删除。此过程可能需要数分钟。

确认网络模块

将新的网络模块安装到机箱时，或将现有模块替换为一个具有不同产品 ID (PID) 的模块时，必须确认网络模块，然后才能开始使用该模块。

过程

步骤 1 进入 `scope fabric-interconnect` 模式：

```
scope fabric-interconnect
```

步骤 2 在安装新模块或用不同类型（即不同PID）的网络模块更换网络模块后，输入 `acknowledge` 命令：

```
acknowledge
```

示例：

```
FPR1 /fabric-interconnect # acknowledge
  fault  Fault
  slot   Card Config Slot Id <=====
```

步骤 3 输入 `acknowledge slot` 以确认插入的插槽。

```
acknowledge slot
```

示例：

```
FPR1 /fabric-interconnect # acknowledg slot 2
  0-4294967295 Slot Id
```

步骤 4 确认配置：

```
commit-buffer
```

使网络模块离线或在线

按照以下步骤以使用 CLI 命令使网络模块离线，或者使其重新恢复在线；在执行模块在线插入和删除 (OIR) 时用于示例。



注释

- 如果要删除或更换网络模块，请按照适用于设备的《安装指南》的“维护和升级”一章中的说明进行操作。请参阅<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>。
- 如果在 8 端口 1G 铜缆 FTW 网络模块 (FPR-NM-8X1G-F FTW) 上执行网络模块在线插入和拆卸 (OIR)，请注意，网络模块 LED 将保持熄灭，直到您使用此程序使卡上线。LED 先闪烁琥珀色，然后在发现网络模块后将更改为绿色，并且应用程序上线。



注释

如果删除 FTW 网络模块并确认插槽，则系统会从威胁防御逻辑设备中删除网络模块端口。在这种情况下，必须先使用管理中心删除硬件旁路内联集配置，然后再重新插入网络模块。重新插入网络模块后，必须执行以下操作：

- 使用 机箱管理器 或 FXOS 命令行界面 (CLI) 将网络模块端口配置为管理在线状态。
- 将网络模块端口添加到威胁防御逻辑设备，并使用管理中心重新配置端口。

如果您在未确认插槽的情况下移除网络模块，则会保留内联集配置，并且端口在管理中心中显示为关闭。重新插入网络模块后，将恢复先前的配置。

有关内联集的硬件旁路的详细信息，请参阅[硬件旁路对](#)。

过程

步骤 1 对于要使其离线的模块，使用以下命令进入 `/fabric-interconnect` 模式，然后进入 `/card` 模式：

```
scope fabric-interconnect a
scope card ID
```

步骤 2 您可以使用 `show detail` 命令来查看关于此卡的信息，包括其当前状态。

步骤 3 要使模块离线，请输入：

```
set adminstate offline
```

步骤 4 输入 `commit-buffer` 命令，以保存配置更改。

您可以再次使用 `show detail` 命令确认该模块已离线。

步骤 5 要使网络模块重新恢复在线，请输入：

```
set adminstate online
commit-buffer
```

示例

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
  Id: 2
  Description: Firepower 4x40G QSFP NM
  Number of Ports: 16
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-NM-4X40G
  HW Revision: 0
  Serial (SN): JAD191601DE
  Perf: N/A
  Admin State: Online
  Power State: Online
  Presence: Equipped
  Thermal Status: N/A
  Voltage Status: N/A
FP9300-A /fabric-interconnect/card # set adminstate offline
FP9300-A /fabric-interconnect/card* # commit-buffer
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
  Id: 2
  Description: Firepower 4x40G QSFP NM
  Number of Ports: 16
  State: Offline
  Vendor: Cisco Systems, Inc.
  Model: FPR-NM-4X40G
  HW Revision: 0
  Serial (SN): JAD191601DE
  Perf: N/A
  Admin State: Offline
  Power State: Off
  Presence: Equipped
  Thermal Status: N/A
  Voltage Status: N/A
FP9300-A /fabric-interconnect/card #
```

刀片运行状况监控

当在刀片上检测到指定数量的意外应用重启时，会在安全模块或引擎上启用故障保护，以防止无限启动循环情况，这可能会对冗余 HA 或集群部署产生进一步的副作用。

刀片平台会定期执行运行状况检查，并将结果报告给 MIO。如果刀片处于故障状态，您将收到故障和错误消息通知。

故障和错误消息

如果刀片存在任何问题，您可以在平台的“概述” (Overview) 页面中查看故障和错误消息。

- “概述” (Overview) 页面 - “安全模块” (Security Module) 会显示运行状态为“故障” (Fault) 的故障符号。
- “安全模块” (Security Module) 页面 - 刀片服务器中的“服务状态” (Service State) 将显示为“故障” (Fault)。将鼠标悬停在“i”图标上时，会显示错误消息。
- “逻辑设备” (Logical Devices) 页面 - 如果逻辑设备可用且安全模块出现故障，则将鼠标悬停在上方时，“i”图标会显示错误消息。



注释 您可以从 FXOS CLI 配置和管理故障保护设置。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。