设备设置

添加设备后，您可以在**设备 (Device)** 页面上编辑与设备相关的设置。

1. 选择**设备** > **设备管理**。
2. 在要修改的设备名单旁，点击 **编辑** ()。
3. 点击**设备 (Device)**。

编辑常规设置

设备 (Device) 页面上的 **常规 (General)** 部分会显示下表所述信息。

图 *1:* 常规

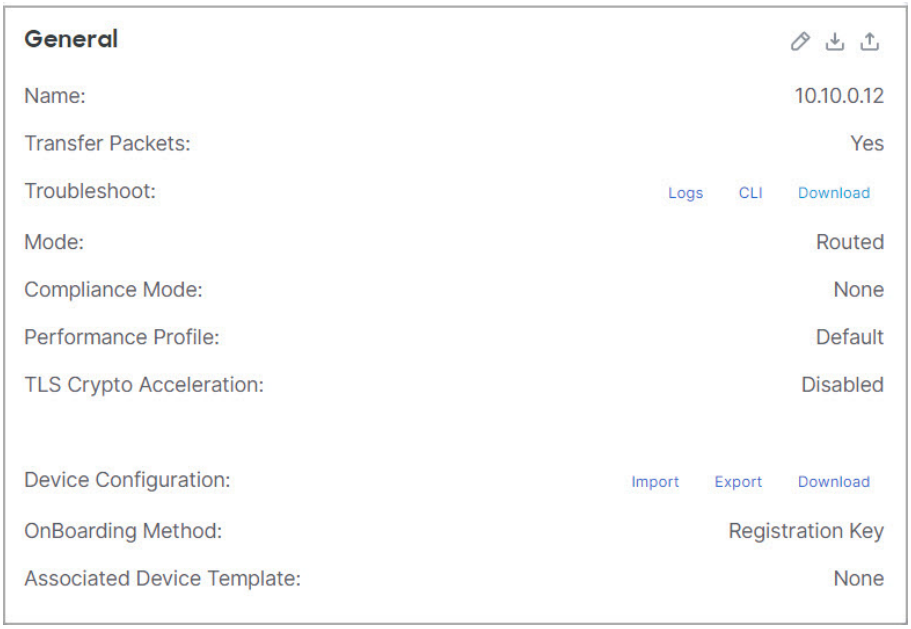


表 *1:* “常规” *(General)* 部分表字段

字段	说明
名称	防火墙管理中心上的设备的显示名称。
传输数据包	显示托管设备是否将数据包数据随事件一起发送到 防火墙管理中心 。
故障排除	可用于生成和下载故障排除文件，还可查看CLI命令输出。请参阅生成故障排除文件 ， 第 3 页和查看 CLI 输出 ， 第 6 页。
模式	显示设备的管理接口的模式：**路由**或**透明**。
合规模式	显示设备的安全认证合规性。有效值为 CC、UCAPL 和 None。
性能配置文件	这将显示设备的核心分配性能配置文件，如平台设置策略中所配置。
TLS 加密加速：	显示 TLS 加密加速是已启用还是已禁用。
设备配置	允许您复制、导出或导入配置。请参阅将配置复制到另一台设备 ， 第 9 页和导出和导入设备配置 ， 第 10 页。
载入方法	显示设备是使用注册密钥还是使用序列号注册的 (零接触调配)。

您可以在此部分编辑其中一些设置。

过程

步骤 1 选择 **设备** > **设备管理**。

步骤 2 在要修改的设备名单旁，点击 **编辑** ()。

步骤 3 点击**设备 (Device)**。

步骤 4 在**常规 (General)** 部分中，点击 **编辑** ()。

a) 输入托管设备的**名称 (Name)**。

b) 选择**转换数据包 (Transfer Packets)** 复选框以允许数据包数据随事件一起存储在 防火墙管理中心 上。

c) 点击**强制部署 (Force Deploy)** 以强制将当前策略和设备配置部署到设备。

注释
强制部署比常规部署需要更多时间，因为它涉及要在Firewall Threat Defense上部署的策略规则的完整生成。

步骤 5 有关 **故障排除** 操作，请参阅 生成故障排除文件，第 3 页 和 查看 CLI 输出，第 6 页。

步骤 6 有关**设备配置** 操作，请参阅将配置复制到另一台设备，第 9 页和导出和导入设备配置，第 10 页。

步骤 7 点击**部署 (Deploy)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

生成故障排除文件

您可以在每个设备以及所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。

您也可以从 **设备** > **设备管理** 触发文件生成，从 **更多** () 下拉列表选择**故障排除文件**。

过程

步骤 1 选择 **设备** > **设备管理**。

步骤 2 点击要查看的设备旁边的 **编辑** ()。

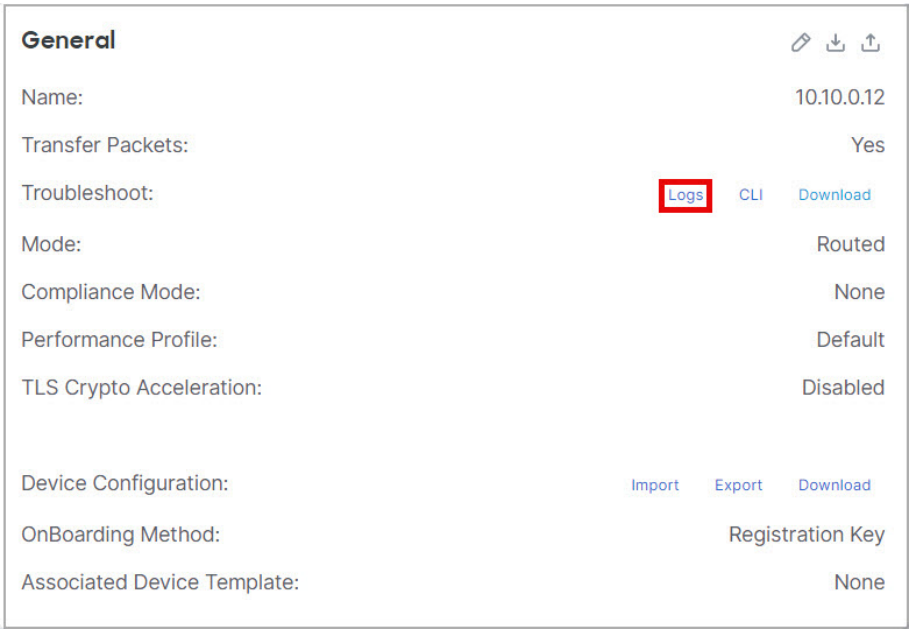
在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备** 或 **集群**。

步骤 4 为设备或所有集群节点生成日志。

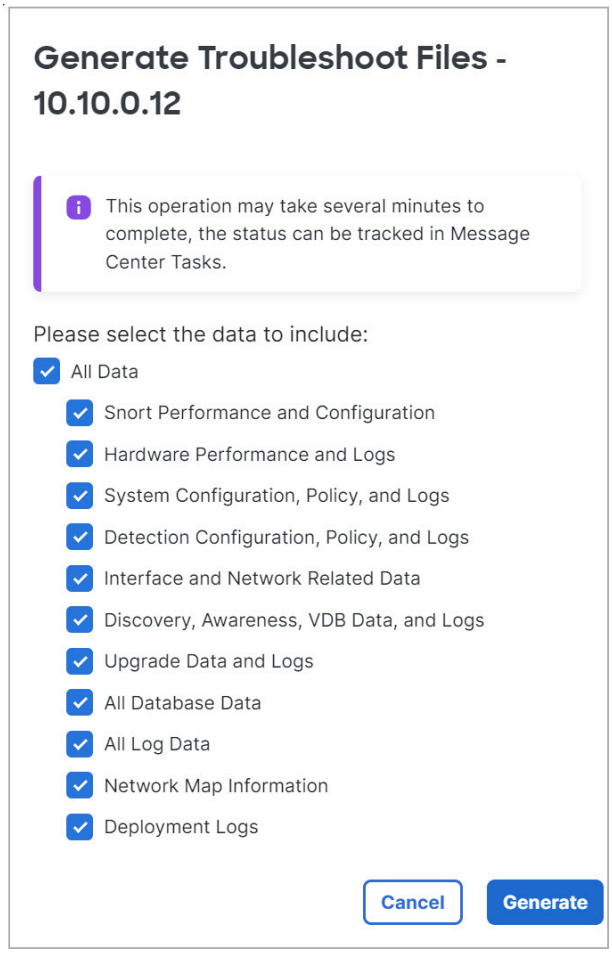
a) 在**常规**区域的**故障排除**部分中，点击**日志**。

图 *2:* 日志



b) 系统会提示您选择要包括的日志。对于集群，在 **设备**下，您可以选择 **所有设备** 或单个节点。集群还具有可用的 **集群日志** 。

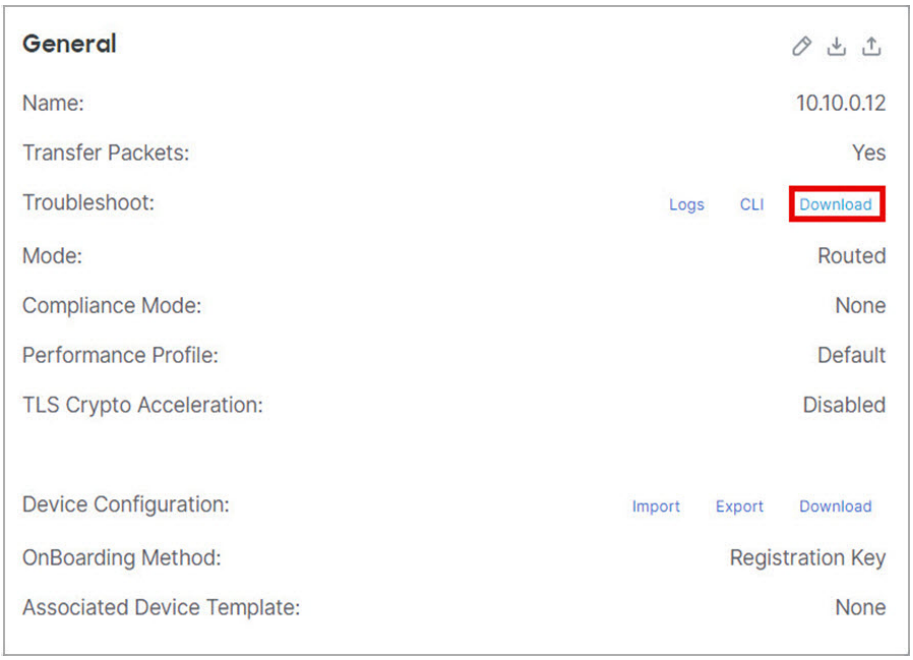
图 *3:* 生成故障排除文件



c) 点击**生成 (Generate)**。

步骤 5 要下载生成的日志，请在**常规**区域**故障排除**部分中，点击**下载**。

图 *4:* 下载



日志将下载到您的计算机。

查看 CLI 输出

您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。

对于设备，执行以下命令：

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

对于集群或集群节点：

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**

- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**
- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

过程

步骤 1 选择 **设备** > **设备管理**。

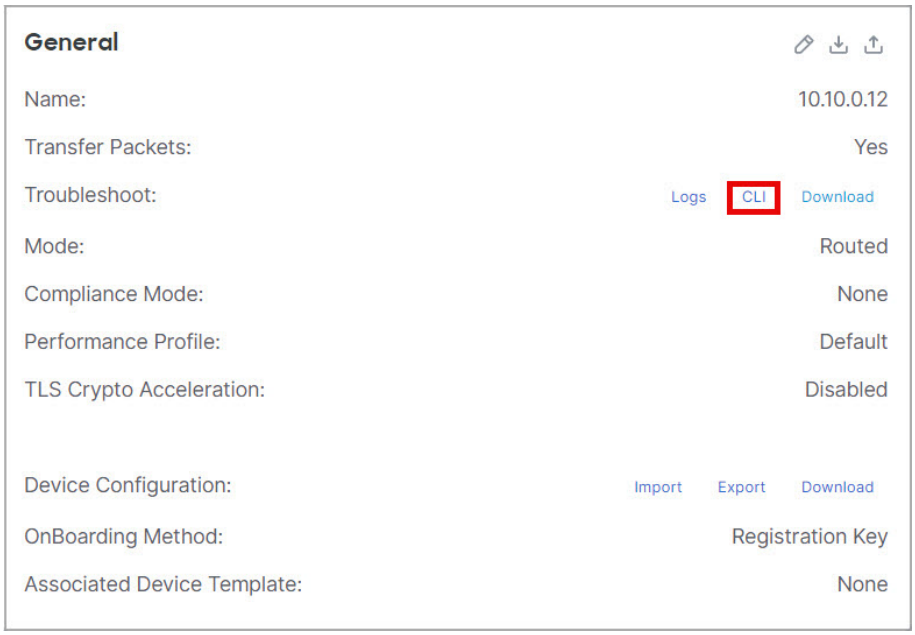
步骤 2 点击要查看的设备旁边的 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备** 或 **集群**。

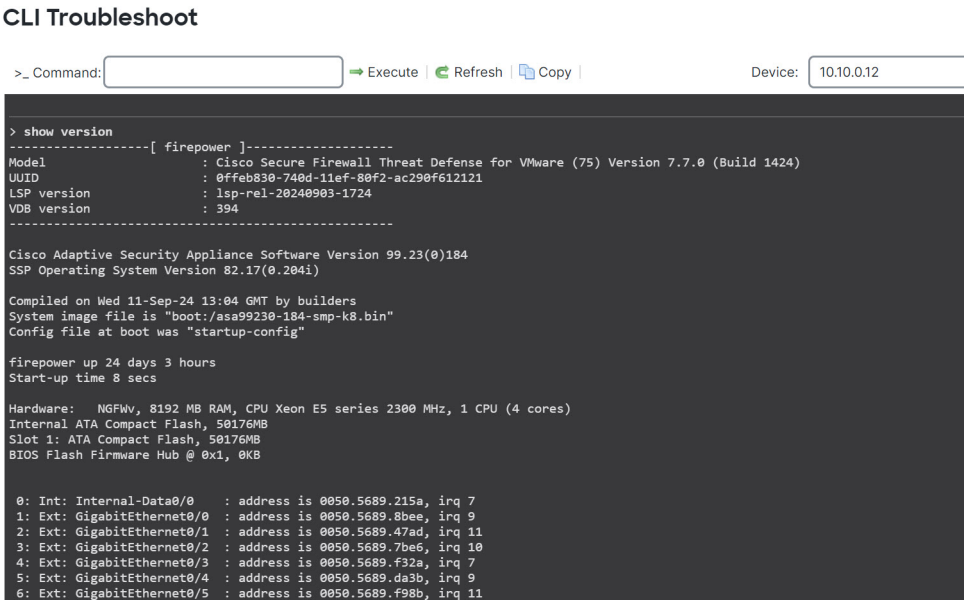
步骤 4 在**常规**区域的**故障排除**部分中，点击 **CLI**。

图 *5: CLI*



系统将显示 **CLI 故障排除** 对话框，其中包含已执行的预定义 CLI。

图 *6: CLI* 故障排除



步骤 5 在 **CLI 故障排除** 对话框中，您可以执行以下任务。

- 在 **命令** 字段中输入 **show** 命令，然后点击 **执行**。新的命令输出将添加到窗口中。
- 点击 **刷新** 以重新运行预定义的 CLI。

- 点击 **复制** 以将输出复制到剪贴板上。
- 对于集群，请从**设备**下拉列表中选择其他节点。

步骤 6 点击**关闭 (Close)**。

将配置复制到另一台设备

在网络中部署新设备时，可以直接复制预配置设备上的配置和策略，而无需手动重新配置新设备。

开始之前

确认：

- 源设备和目标设备是相同型号，并且运行相同版本的软件。
- 源是独立设备或高可用性对。
- 目标设备是独立设备。
- 源设备和目标设备具有相同数量的物理接口。
- 源设备和目标设备处于相同的防火墙模式：路由或透明。
- 源设备和目标设备处于相同的安全认证合规模式。
- 源设备和目标设备处于相同的域。
- 源设备或目标设备上均未进行配置部署。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要修改的设备名单旁，点击 **编辑** (✎)。

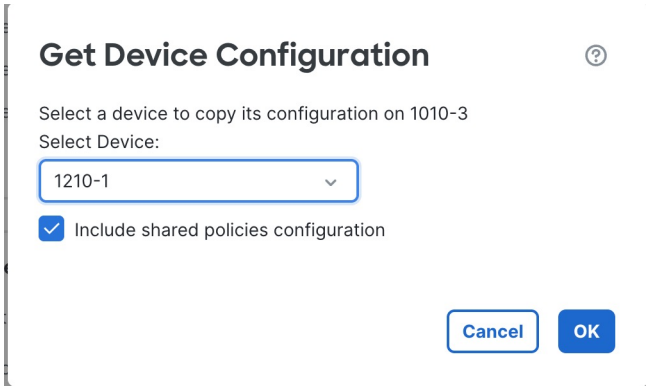
步骤 3 点击 **设备**。

步骤 4 在**常规**部分中，执行以下操作之一：

图 7: 复制或推送设备配置

- 点击 **获取设备配置** (⬇) 以将设备配置从其他设备复制到新设备。在**获取设备配置**页面中，从**选择设备**下拉列表中选择源设备。

图 *8:* 选择设备



- 点击 **推送设备配置** (⬆) 以将设备配置从当前设备复制到新设备。在 **推送设备配置** 页面上，从 **目标设备**下拉列表中选择复制配置的目标设备。

步骤 5 （可选）选中**包括共享策略配置 (Include shared policies configuration)** 复选框以复制策略。

共享策略（例如访问控制策略、NAT、平台设置和 FlexConfig 策略）可在多个设备之间共享。

步骤 6 点击**确定 (OK)**。

您可以在消息中心中的 **任务 (Tasks)** 监控复制设备配置任务的状态。

复制设备配置任务发起后，便会擦除目标设备上的配置，并将源设备的配置复制到目标设备。

警告 完成复制设备配置任务后，无法将目标设备还原为其原始配置。

导出和导入设备配置

注释

- 共享策略和设备策略不支持在本地 防火墙管理中心 和 云交付的防火墙管理中心 (cdFMC) 之间导出和导入设备配置。
- 如果在不同的丢弃中为策略更改了基础模型，则丢弃版本不支持 cdFMC 的导出和导入云交付的防火墙管理中心。
- 只有当设备 UUID、型号和版本相同时，才支持导出和导入设备配置。

您可以导出设备页面上可配置的所有设备特定配置，包括：

- 接口
- 内联集

- 路由
- DHCP
- VTEP
- 关联对象

然后，您可以在以下使用案例中为同一设备导入已保存的配置：

- 将设备移动到其他 防火墙管理中心 — 首先从原始 防火墙管理中心 取消注册设备，然后将设备添加到新的 防火墙管理中心。然后，您可以导入保存的配置。
- 在域之间移动设备 - 在域之间移动设备时，不会保留某些设备特定的配置，因为新域中不存在支持对象（例如安全区域的接口组）。通过在域移动后导入配置，将为该域创建任何必要的对象，并恢复设备配置。
- 恢复旧配置 - 如果部署的更改会对设备的运行产生负面影响，则可以导入已知工作配置的备份副本，以恢复以前的运行状态。
- 重新注册设备 - 如果从 防火墙管理中心 中取消注册设备，但随后想要重新添加，则可以导入已保存的配置。

请参阅以下准则：

- 您只能将配置导入到同一设备（UUID 必须匹配）。您无法将配置导入到其他设备，即使是同一型号也是如此。
- 请勿在导出和导入的间隙更改设备上运行的版本；版本必须匹配。
- 如果在导出后更改资产（例如添加或删除网络模块，或配置或加入分支端口）， 防火墙管理中心则设备资产将不匹配 。在这种情况下，当您尝试部署时，系统将维护设备资产，并且系统会提示您同步接口（请参阅 与 防火墙管理中心同步接口更改）并丢弃 防火墙管理中心 中不兼容的配置。您必须在 防火墙管理中心中重复执行资产更改和相关配置。
- 如果导出独立配置，则无法将其导入到高可用性对，反之亦然。
- 将设备移至其他 防火墙管理中心 时，目标 防火墙管理中心 版本必须与源版本相同。
- 如果对象不存在，系统将创建该对象。如果对象存在，但值不同，请参阅下文：

表 *2:* 对象导入操作

场景	导入操作
存在具有相同名称的对象。	重用现有对象。
存在名称相同但值不同的对象。	网络和端口对象：为此设备创建对象覆盖。请参阅对象覆盖。 接口对象：创建新对象。例如，如果类型（安全区域或接口组）和接口类型（例如，路由或交换）不匹配，则会创建新对象。 所有其他对象：即使值不同，也可重复使用现有对象。

场景	导入操作
对象不存在。	创建新对象。

过程

步骤 1 选择**设备** > **设备管理**。

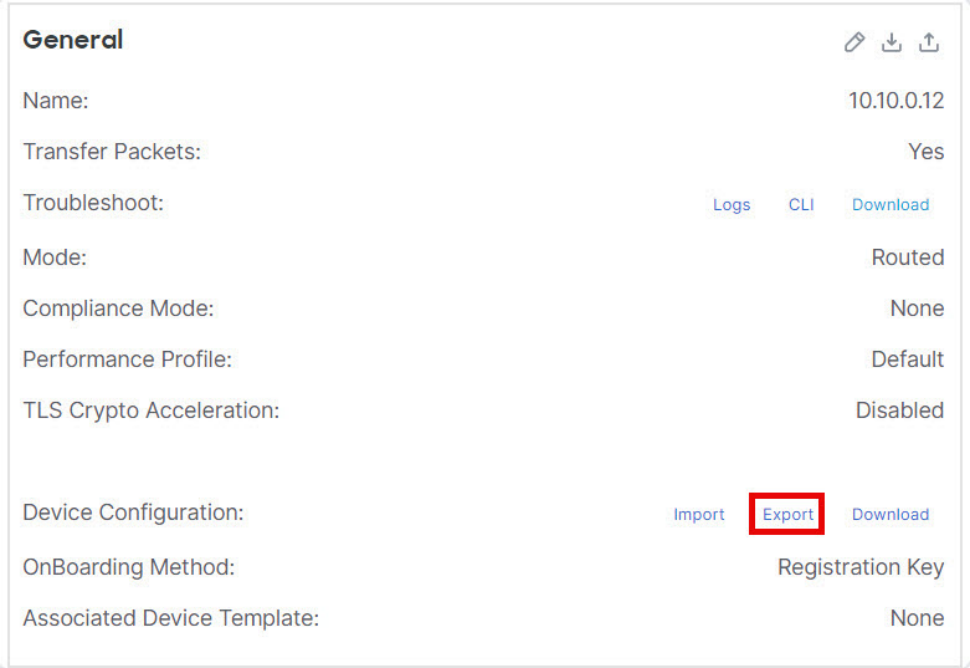
步骤 2 在要编辑的设备旁边，点击 **编辑** ()。

步骤 3 点击**设备 (Device)**。

步骤 4 导出配置。

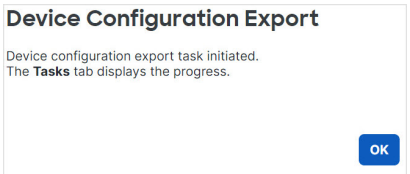
a) 在**常规 (General)** 区域，点击**导出 (Export)**。

图 *9:* 导出设备配置



系统将提示您确认导出；点击**确定**。

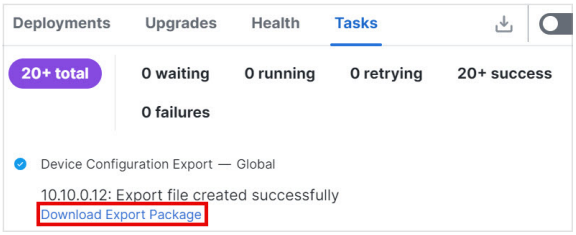
图 *10:* 确认导出



您可以在**任务 (Tasks)** 页面中查看导出进度。

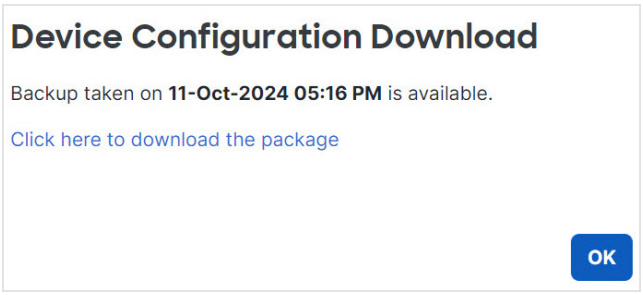
b) 点击 **通知**，然后点击“**任务**”选项卡。验证导出是否已完成，然后点击 **下载导出包 (Download Export Package)**。或者，您可以点击**常规 (General)** 区域中的**下载 (Download)** 按钮。

图 *11:* 导出任务



系统将提示您下载软件包；点击**点击此处下载软件包 (Click here to download the package)** 以本地保存文件，然后点击**确认 (OK)** 以退出对话框。

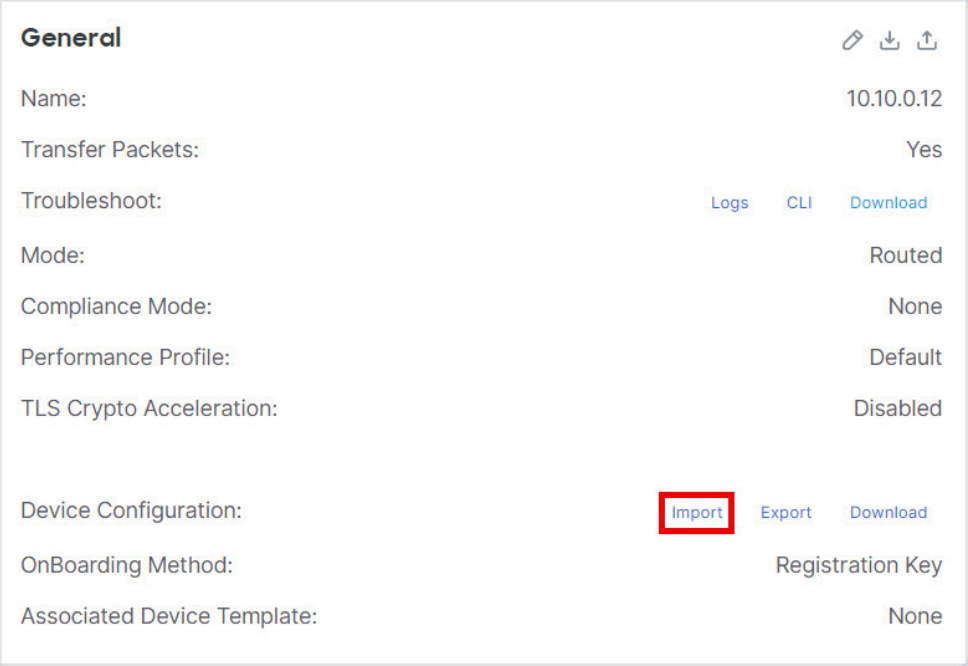
图 *12:* 下载软件包



步骤 5 导入配置。

a) 在**常规 (General)** 区域中，点击**导入 (Import)**。

图 *13:* 导入设备配置



系统将提示您确认将替换当前配置。点击**是 (Yes)**，然后导航到配置包（使用后缀 .sfo；请注意，此文件与备份/恢复文件不同）。

图 *14:* 导入软件包

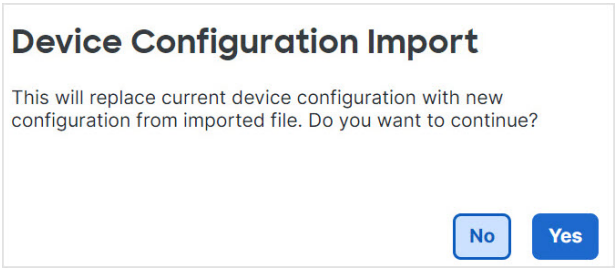
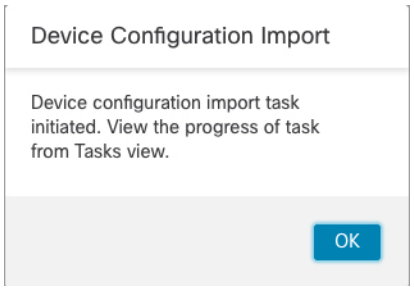


图 *15:* 导航至软件包

系统将提示您确认导入；点击**确认 (OK)**。

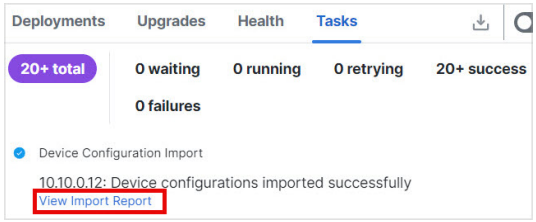
图 *16:* 确认导入



您可以在**任务 (Tasks)** 页面中查看导入进度。

b) 要查看导入报告以便查看导入的内容，请点击 **通知**，然后点击 **任务** 选项卡。点击**查看导入报告**。

图 *17:* 查看导入报告



设备配置导入报告 (Device Configuration Import Reports) 页面提供可用报告的链接。

Device	Shared Policies	Device Configurations
0ffeb830-740d-11ef-80f2-ac290f612121	Report does not exist	Device configurations import report

c) 部署配置更改；请参阅 部署配置更改。

编辑许可证设置

设备 (Device) 页面的**许可证 (License)** 部分显示为设备启用的许可证。

如果在防火墙管理中心上有可用的许可证，则可以启用设备上的许可证。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要启用或禁用许可证的设备旁边，点击 **编辑** ()。

步骤 3 点击**设备**。

步骤 4 在**许可证 (License)** 部分中，点击 **编辑** ()。

步骤 5 选中或取消选中要为托管设备启用或禁用的许可证旁边的复选框。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

查看系统信息

设备页面的**系统**部分显示一个只读表格，其中包含系统信息，如下表所述。

您也可以使用右上角的图标从此窗格关闭或重启设备。

图 *18:* 系统

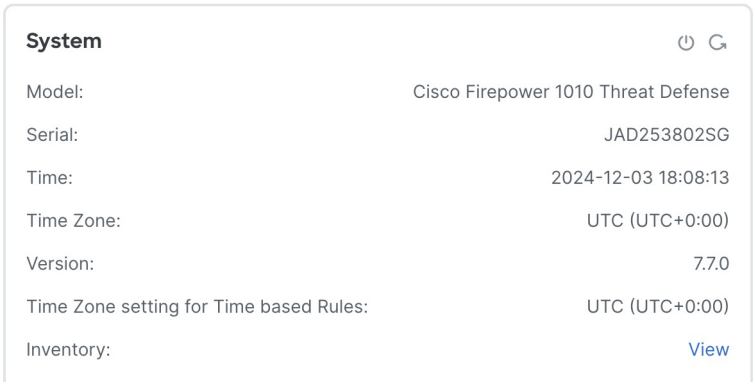


表 *3:* 系统部分表字段

字段	说明
关闭设备 ()	关闭设备。请参阅关闭或重新启动设备。
重启设备 ()	重新启动设备。请参阅关闭或重新启动设备。
型号	型号名称和编号。
系列	PCB（电路板）序列号。防火墙包含两个序列号：机箱序列号和PCB序列号。机箱序列号显示在清单部分中。
时间	设备的当前系统时间。
时区	时区。
版本	托管设备上当前安装的软件版本。

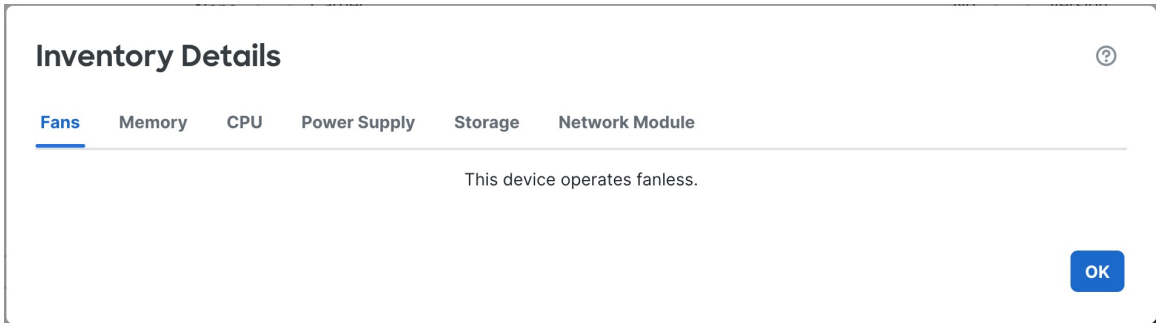
字段	说明
基于时间的规则的时区设置	设备在设备平台设置中指定的时区下的当前系统时间。
设备清单	清单详细信息。请参阅查看设备清单。

查看设备资产

点击**系统**部分中**清单**旁边的**查看**，查看设备清单信息表格，包括风扇、内存、CPU、电源、存储和网络模块。

清单详细信息表格显示分配了产品标识符 (PID) 的 Firewall Threat Defense 设备中安装的所有思科产品的信息。PID 是可用于订购产品的产品名称。

图 *19:* 设备清单详细信息



清单详细信息表格的**内存**选项卡显示受支持 Firewall Threat Defense 设备的现场可更换内存模块信息。它还包括内存模块的运行终端安全评估，这有助于提高其现场可维护性。状态可以是以下其中一项：

- **可操作**：表示现场可更换内存模块已安装在 Firewall Threat Defense 设备中，且容量符合设备平台的预期容量。
- **已降级**：表示已安装内存模块的容量与 Firewall Threat Defense 设备平台的预期容量不匹配，或检测到不可纠正的错误。如需进一步帮助，请联系思科技术支持中心。
- **无法操作**：表示 Firewall Threat Defense 设备无法检测到双列直插内存模块。

查看检测引擎

设备 (Device) 页面的“检测引擎”(Inspection Engine) 部分会显示。Snort 3 是唯一可用于 7.7 及更高版本设备的引擎。

注释 Snort3 是 Cisco Secure Firewall 1200 的默认配置。它不支持 Snort2。

编辑运行状况设置

设备 (Device) 页面上的**运行状况 (Health)** 部分显示下表所述信息。

图 *20:* 运行状况

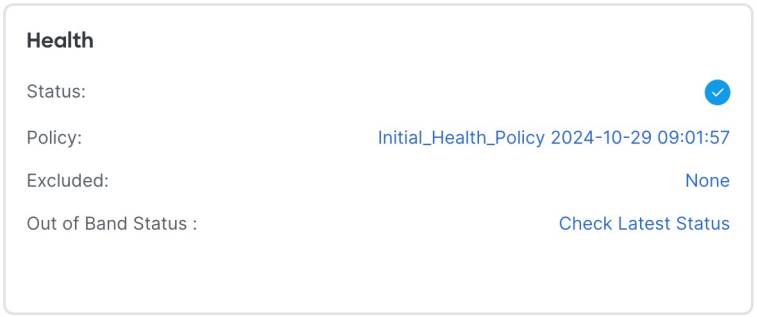


表 *4:* 运行状况部分表字段

字段	说明
状态	一个代表设备当前运行状况的图标。点击该图标将显示设备 的“运行状况监控器”(Health Monitor)。
策略	一个指向当前部署在设备 上的运行状况策略的只读版本的链接。
已排除	一个指向**运行状况排除 (Health Exclude)** 页面 的链接，您可以在该页面上启用和禁用运行状况排除模块。
带外状态	指向**带外配置详细信息 (Out-of-Band configuration details)** 对话框的链接，您可以在其中查看在设备CLI上所做的带外配置更改。在下一次部署之前，您必须确认配置差异，并手动匹配要保留在 防火墙管理中心 中的任何更改。请参阅带外配置检测 ，第 18 页。

带外配置检测

如果断开了与设备的管理连接，您可以直接通过设备 CLI 选择配置更改：

- 如果使用数据接口进行管理器访问，则恢复管理连接
- 选择无法等到连接恢复后再进行的配置更改

⚠

注意 您应该知道恢复或紧急使用时所需的命令。请勿使用此功能来尝试更改配置。如果您不知道哪些命令是必需的，或者不确定某个命令的作用，建议您联系思科技术支持中心以寻求指导。

在恢复管理连接后，防火墙管理中心 将检测设备上的配置更改。它不会自动更新 防火墙管理中心 中的设备配置；您必须查看配置差异，确认设备配置不同，然后在部署之前在防火墙管理中心 中手动进行相同的更改。

注意 在确认后部署时，防火墙管理中心 配置中不存在的任何配置将在设备上覆盖。

带外配置准则

恢复配置模式下支持的功能区域

您可以在恢复配置模式下在诊断 CLI 中配置以下功能区域：

- 接口
- 静态路由
- 动态路由：BGP 和 OSPF
- 预过滤器
- 站点间 VPN
- NAT

与其他诊断 CLI 命令一样，有关每个命令的详细信息，请参阅 ASA 命令参考 。

不支持的功能

- 在多实例模式下不支持。
- 不能添加或删除 EtherChannel。

高可用性和群集

- 恢复配置模式仅在主用/控制节点上可用。
- 在集群控制链路或故障转移链路的恢复配置模式下，不支持以下接口命令：
  - **duplex**
  - **fec**
  - **negotiate-auto**
  - **shutdown**
  - **speed**
- 如果在您退出恢复配置模式会话之前发生故障转移或集群切换，防火墙管理中心 将不会检测新的主用/控制节点上的更改。我们建议在新的主用/控制节点上重新进入恢复配置模式，并进行小

幅更改以触发发现功能之前的所有更改。否则，如果您没有手动匹配 防火墙管理中心中的更改，则这些更改将在部署时被覆盖，而不发出任何通知。

- 如果在主用/控制节点上进行带外配置更改，但在配置同步之前，高可用性/集群最终处于“裂脑”模式（在这种情况下，多个节点由于或故障转移/集群控制链路故障时），则当高可用性/集群恢复正常运行且另一个节点变为主用/控制状态时，配置更改将会丢失。
- 如果有活动恢复配置模式会话，则在退出该会话之前，新节点无法加入或重新加入高可用性/集群。

NAT

- 通过恢复配置模式，可以创建如下重叠 PAT 池规则：

  nat (eth_12_subintf_one,any) source dynamic any pat-pool pat_pool_4

  nat (eth_12_subintf_one,any) source dynamic any pat-pool pat_pool_4 include-reserve

  防火墙管理中心 不允许此重叠。如果目的是将 **include-reserve** 添加到现有 NAT 规则中，请首先使用 **no** 命令删除该规则，然后使用 **include-reserve** 选项重新添加该规则。

- 如果在恢复配置模式下创建服务对象以用于如下所示的 NAT 规则中：

  object service obj_mapped_svc

  service tcp source eq www

  object service obj_real_svc

  service tcp source eq 7080

  nat (any,any) source dynamic obj_two obj_dyn_host service obj_real_svc obj_mapped_svc

  然后，当在 防火墙管理中心中重新创建规则时， 防火墙管理中心 会将服务对象名称替换为自动生成的名称。由于 NAT 规则在部署时不匹配，因此系统将在应用新的 防火墙管理中心 规则之前删除 recovery-config 模式规则，从而导致少量流量中断。

其他准则

- 要修改现有的规则或路由，应使用命令的 **no** 形式删除现有命令，然后重新添加已修改的规则。此方法可避免冲突和错误。例如：

  不正确：

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
  center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
  or
to restore manager access. Do not change management center's auto-generated
configurations.

 After your management center is reachable, manually make the same configuration changes
  in the
```

```
management center. The management center cannot implement them automatically. When you
 deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
 node join
will be blocked till config CLI session is active, so make sure to exit from the config
 CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: ccfc11a8 4e46d55e 0c99b5ae 3b18a8f1

3939 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

这种情况下会添加第二个路由，而不是替换第一个路由。

正确：

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
 center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
 or
to restore manager access. Do not change management center's auto-generated
configurations.

 After your management center is reachable, manually make the same configuration changes
 in the
management center. The management center cannot implement them automatically. When you
 deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
 node join
will be blocked till config CLI session is active, so make sure to exit from the config
 CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# no route outside 10.0.0.0 255.0.0.0 20.1.1.1
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: 81bcc51d 43771bbd 15b6dde6 afeb3442

3945 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

- 如果您启用了自动回滚（请参阅 编辑部署设置，第 75 页），并且由于部署而丢失管理连接，则不应启动带外配置。而是等待 20 分钟，以便自动回滚到先前的部署，或者在 CLI 中使用

configure policy rollback 命令手动回滚（请参阅如果防火墙管理中心断开连接，则手动回滚配置，第 63 页）。如果管理连接仍然关闭，自动回滚将覆盖带外配置更改。

- 对于预过滤器规则，我们不建议添加全新的规则（使用 **access-control advanced** 命令）；将预过滤器规则与入侵策略和日志记录的集成需要 防火墙管理中心，它生成规则 ID 并将其与其他策略集成。
- 所有恢复配置模式会话都将以用户名“enable_15”记录在系统日志中。

访问诊断 CLI 中的恢复配置模式

当管理连接断开时，您可以使用诊断 CLI 恢复配置模式进行带外配置更改。请确保在 防火墙管理中心中进行相同的更改；本地更改将始终被 防火墙管理中心 部署覆盖。

要实现高可用性和集群，请在主用/控制节点上进行更改。在多实例模式下不支持此模式。

过程

步骤 1 通过控制台端口或使用 SSH 连接至设备 CLI。

请参阅登录到设备的命令行界面。

步骤 2 访问诊断 CLI。

system support diagnostic-cli

enable（当系统提示时，请按 Enter 键，无需输入密码。）

示例：

```
> system support diagnostic-cli
firepower> enable
Password:
```

步骤 3 显示当前运行配置，以供参考。

show running-config

注释
您不能在恢复配置模式下输入 **show** 命令。

步骤 4 进入恢复配置模式。

configure recovery-config

示例：

```
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
 or
to restore manager access. Do not change management center's auto-generated configurations.
```

```
 After your management center is reachable, manually make the same configuration changes
in the
management center. The management center cannot implement them automatically. When you
deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
node join
will be blocked till config CLI session is active, so make sure to exit from the config CLI
 after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)#
```

步骤 5 您现在可以输入选定的配置命令。

输入 **?** 以查看可用的命令。

有关受支持的功能区域，请参阅带外配置准则，第 19 页。

有关命令的详细信息，请参阅 ASA 配置指南或命令参考。

提示
记录所有更改过的命令。虽然防火墙管理中心将稍后显示差异，但最好记录命令更改，以防需要反复更改来恢复管理连接。

示例：

```
firepower(recovery-config)# ?

  access-list            Configure an access control element
  as-path                BGP autonomous system path filter
  bfd                    BFD configuration commands
  bfd-template           BFD template configuration
  cluster                Cluster configuration
  community-list         Add a community list entry
  crypto                 Configure IPSec, ISAKMP, Certification authority, key
  end                    Exit from configure mode
  exit                   Exit from config mode
  extcommunity-list      Add a extended community list entry
  group-policy           Configure or remove a group policy
  interface              Select an interface to configure
  ip                     Configure IP address pools
  ipsec                  Configure transform-set, IPSec SA lifetime and PMTU
                         Aging reset timer
  ipv6                   Configure IPv6 address pools
  ipv6                   Global IPv6 configuration commands
  isakmp                 Configure ISAKMP options
  jumbo-frame            Configure jumbo-frame support
  mac-address            MAC address options
  management-interface   Management interface
  mtu                    Specify MTU(Maximum Transmission Unit) for an interface
  nat                    Associate a network with a pool of global IP addresses
  no                     Negate a command or set its defaults
  object                 Configure an object
  object-group           Create an object group for use in 'access-list', etc
  policy-list            Define IP Policy list
  prefix-list            Build a prefix list
  route                  Configure a static route for an interface
  route-map              Create route-map or enter route-map configuration mode
```

```
  router                Enable a routing process
  sla                   IP Service Level Agreement
  sysopt                Set system functional options
  time-range            Define time range entries
  tunnel-group          Create and manage the database of connection specific
                        records for IPSec connections
  vpdn                  Configure VPDN feature
  vrf                   Configure a VRF
  zone                  Create or show a Zone
firepower(recovery-config)#
```

步骤 6 退出恢复配置模式，系统将提示您保存更改。输入 **exit** 以退出每个子模式，直到您返回启用模式。

您可以选择将更改保存到启动配置，或不保存，仅将更改保留在运行配置中。重新启动后不会保留运行配置更改。如果您稍后进行其他更改并决定保存配置，则先前的所有更改也会保存，因为会保存整个运行配置。

当恢复配置模式会话打开时，部署将被阻止。

示例：

```
firepower(recovery-config)# interface Ethernet0/1
firepower(config-if)# ip address 10.0.0.2 255.0.0.0
firepower(config-if)# exit
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o: y

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#

Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o:

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#
```

步骤 7 依次键入 Ctrl+a 和 d 返回 Firewall Threat Defense CLI，或者输入 **exit** 退出每种模式。

注释
如果您键入 Ctrl+a，然后键入 d 以返回 Firewall Threat Defense CLI，无需先退出恢复配置模式，恢复配置模式会话将保持打开，并且部署将被阻止。

示例：

```
firepower# exit

Logoff

User enable_1 logged in to firepower
Logins over the last 1 days: 4.  Last login: 20:42:51 UTC Dec 4 2024 from console
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> exit
Console connection detached.
>
```

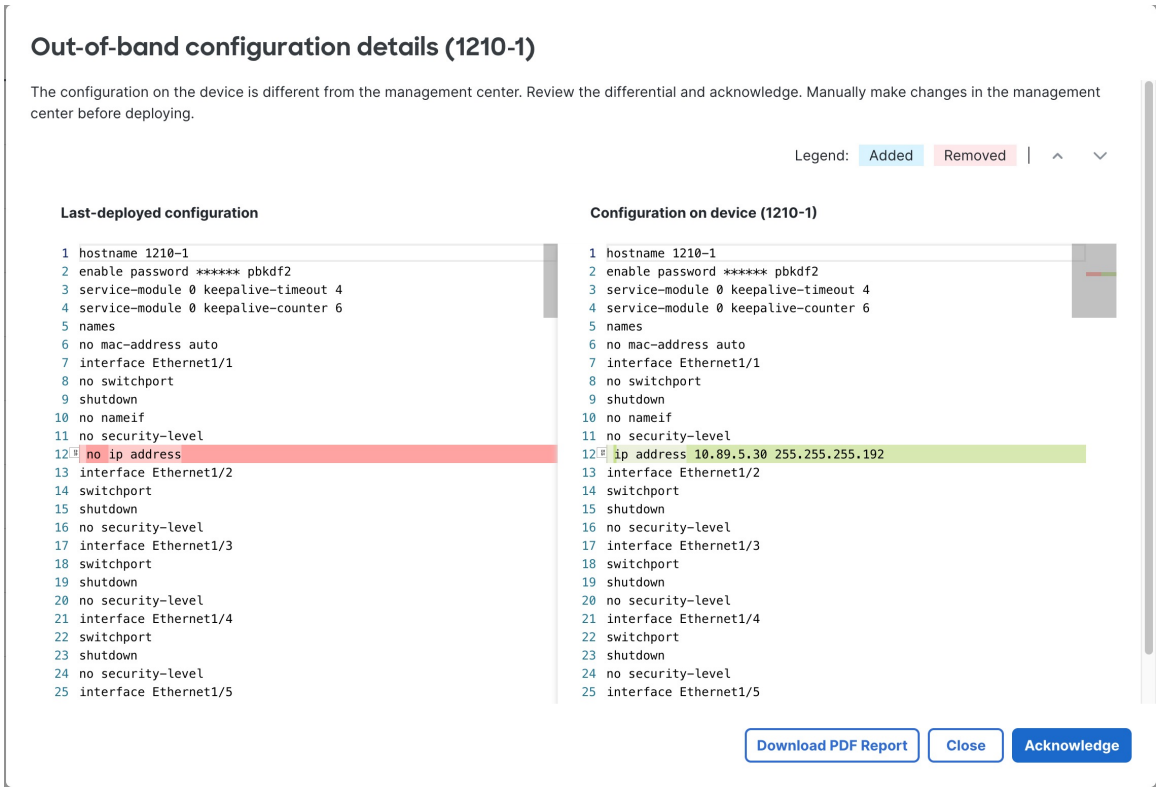
确认带外配置

当 防火墙管理中心 检测到设备上的带外配置更改时，您必须确认更改并与要保留的 防火墙管理中心 中的配置进行匹配。在确认更改之前，部署将被阻止。

过程

步骤 1 打开**带外配置详细信息 (Out-of-Band configuration details)** 对话框。

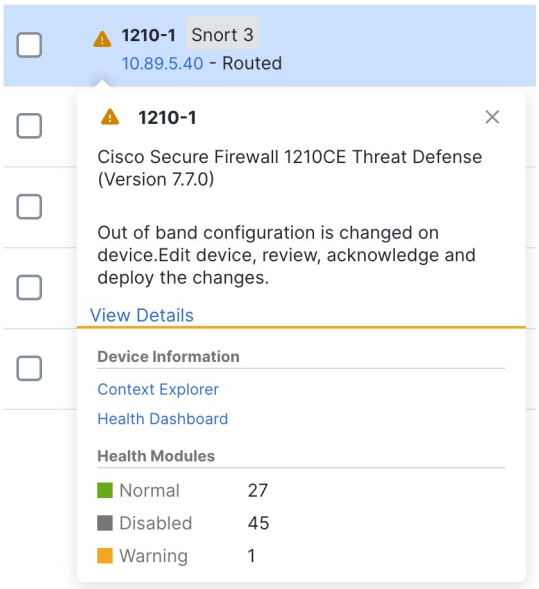
图 *21:* 带外配置详细信息



注释
某些命令在设置为默认值时不会出现在命令输出中。但是，非默认命令会在两侧显示为绿色（添加）或红色（删除）。例如，如果在恢复配置模式下将 **no shutdown** 添加到接口，则 **shutdown** 命令将在左侧 **Last-deployed configuration** 窗格中显示为红色，而右侧 **Configuration on device** 窗格中不会显示 **no shutdown**。在这种情况下，虽然接口的默认设置为 **shutdown**，但解析器会将 **no shutdown** 视为默认设置，并且不会显示它。

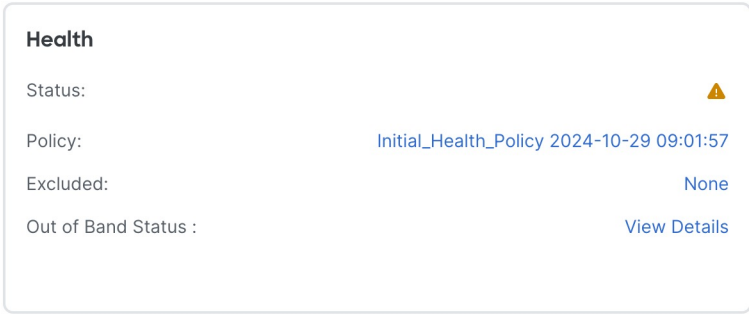
您可以从多个位置打开此对话框。例如，在 **设备 > 设备管理** 页面上，设备将显示一条警告。点击**查看详细信息**。

图 *22:* 设备管理警告



或者，从 **设备** > **设备管理** 导航至**设备**选项卡下的**运行状况**磁贴，您可以点击**查看详细信息**。

图 *23:* 运行状况带外状态



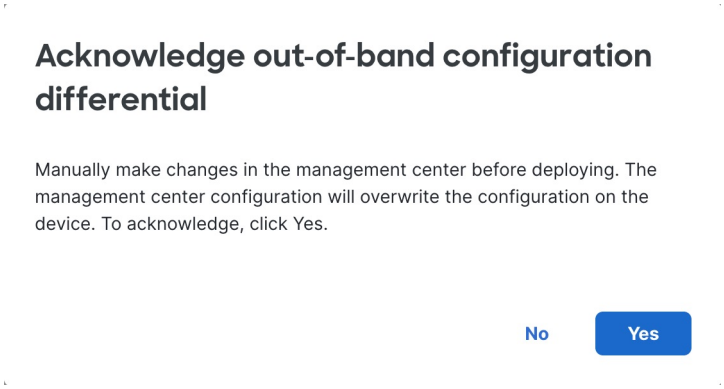
注释
如果带外通知尚未到达 防火墙管理中心，则可以使用**检查最新状态**链接来检查更改。

步骤 2 点击**下载 PDF 报告 (Download PDF Report)**，以便在关闭对话框后参阅需要进行的配置更改。

您也可以随时打开对话框查看更改。

步骤 3 点击**确认**，然后点击**是**。

图 *24:* 确认

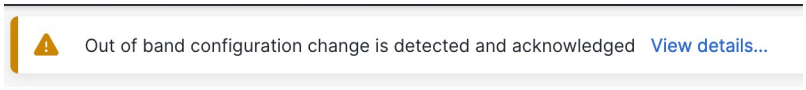


如果要在进行配置更改之前防止意外部署，您可以进行更改，然后返回并点击**确认 (Acknowledge)**。

步骤 4 点击**带外配置详细信息 (Out-of-Band configuration details)** 对话框中的**关闭 (Close)**。

在部署之前，您仍可以重新访问对话框，以便查看需要进行的更改。“设备”(Device) 页面上的状态会发生变化，以显示您已确认带外配置：

图 *25:* 确认状态

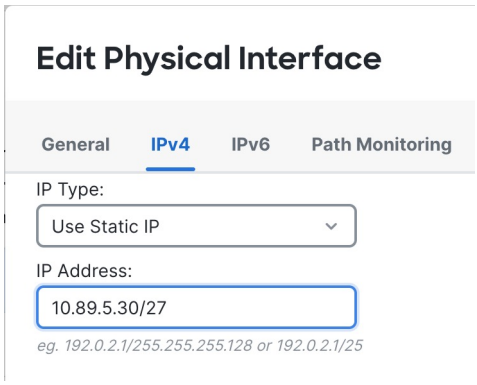


步骤 5 进行您在 CLI 中所做的配置更改。

您需要将配置 CLI 与 防火墙管理中心 屏幕相匹配；CLI 更改不会直接链接到屏幕。

如果不想保留更改，您可以直接部署并覆盖设备配置。您应该进行所有必要的更改，以保持管理连接以及想要保留的任何其他更改。例如，如果在CLI中更改了 IP 地址，则需要转至**接口 (Interfaces)** 页面，编辑接口，并将该 IP 地址设置为匹配：

图 *26:* 匹配 *IP* 地址更改



没有检查机制来确认您是否做了相同的更改；如果需要，您可以设置不同的 IP 地址。

步骤 6 部署配置更改；请参阅 部署配置更改。

在部署后，您可以在 **事件和日志** > **分析** > **审核日志** 页面上查看配置差异，确认是否进行了更改。检查名为设备 *(Device)* > 设备管理 *(Device Management)* > 带外更改 *(Out of band changes)* 的子系统。

编辑管理设置

这些设置控制 防火墙管理中心 与设备建立管理连接的方式。

配置冗余管理器访问数据接口

在使用数据接口进行管理器访问时，您可以配置辅助数据接口，以便在主接口发生故障时接管管理功能。您只能配置一个辅助接口。设备会使用 SLA 监控来跟踪包含两个接口的静态路由和 ECMP 区域的可行性，以便管理流量可以使用这两个接口。

开始之前

- 辅助接口需要与主接口位于不同的安全区域。
- 适用于辅助接口的所有要求与适用于主接口的要求相同。请参阅使用Firewall Threat Defense数据接口进行管理。

过程

步骤 1 在 **设备** > **设备管理** 页面，点击设备的 **编辑** ()。

步骤 2 启用对辅助接口的管理器访问。

此设置是标准接口设置（例如启用接口、设置名称、设置安全区域和设置静态 IPv4 地址）的补充。

a) 选择**接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **管理器访问 (Manager Access)**。
b) 选中**在此接口上为管理器启用管理 (Enable management on this interface for the Manager)**。
c) 点击**确定 (OK)**。

两个接口都会在列表中显示（**管理器访问**）。

图 *27:* 接口列表

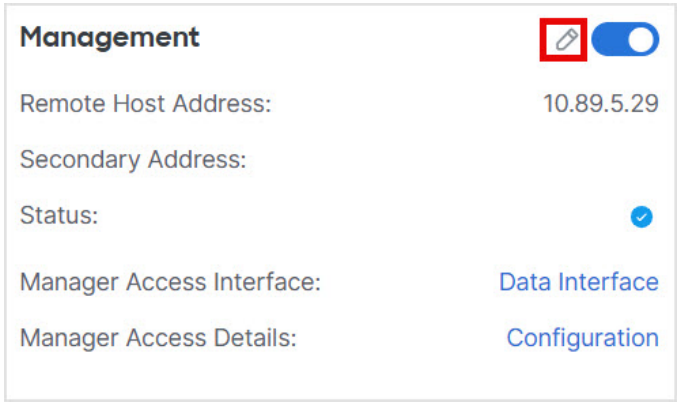
Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

步骤 3 将辅助地址添加到**管理 (Management)** 设置。

a) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

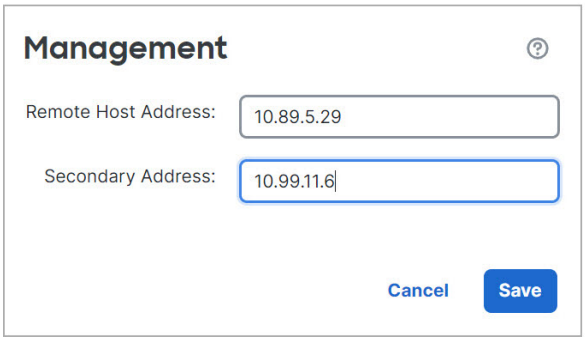
b) 点击**编辑** (✎)。

图 *28:* 编辑管理地址



c) 在**管理 (Management)** 对话框中，在**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址

图 *29:* 管理 *IP* 地址

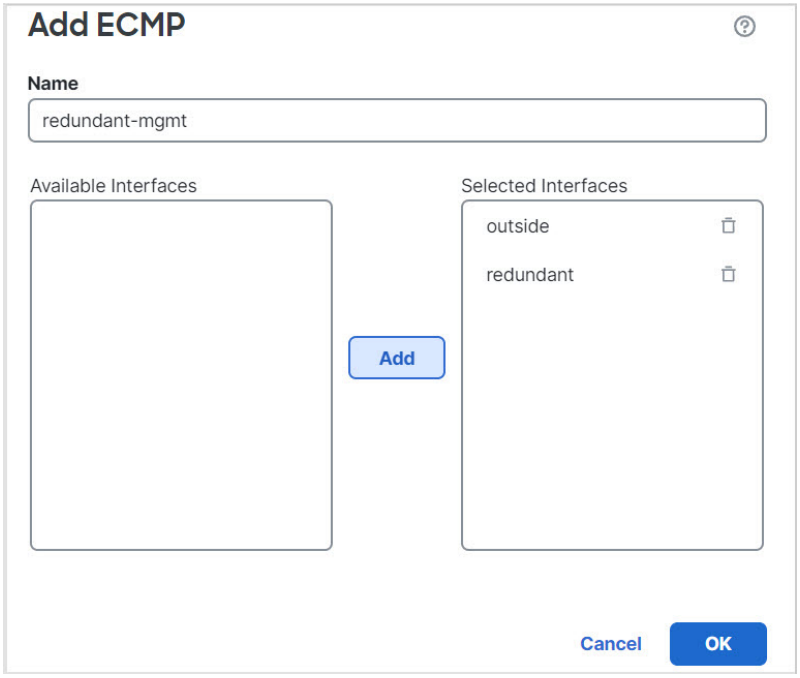


d) 点击**保存 (Save)**。

步骤 4 通过两个接口创建 ECMP 区域。

a) 点击**路由 (Routing)**。
b) 从虚拟路由器下拉列表中，选择主接口和辅助接口所在的虚拟路由器。
c) 点击 **ECMP**，然后点击**添加 (Add)**。
d) 为 ECMP 区域输入一个**名称**。
e) 在**可用接口 (Available Interfaces)** 框下选择主和辅助接口，然后点击**添加 (Add)**。

图 *30:* 添加 *ECMP* 区域

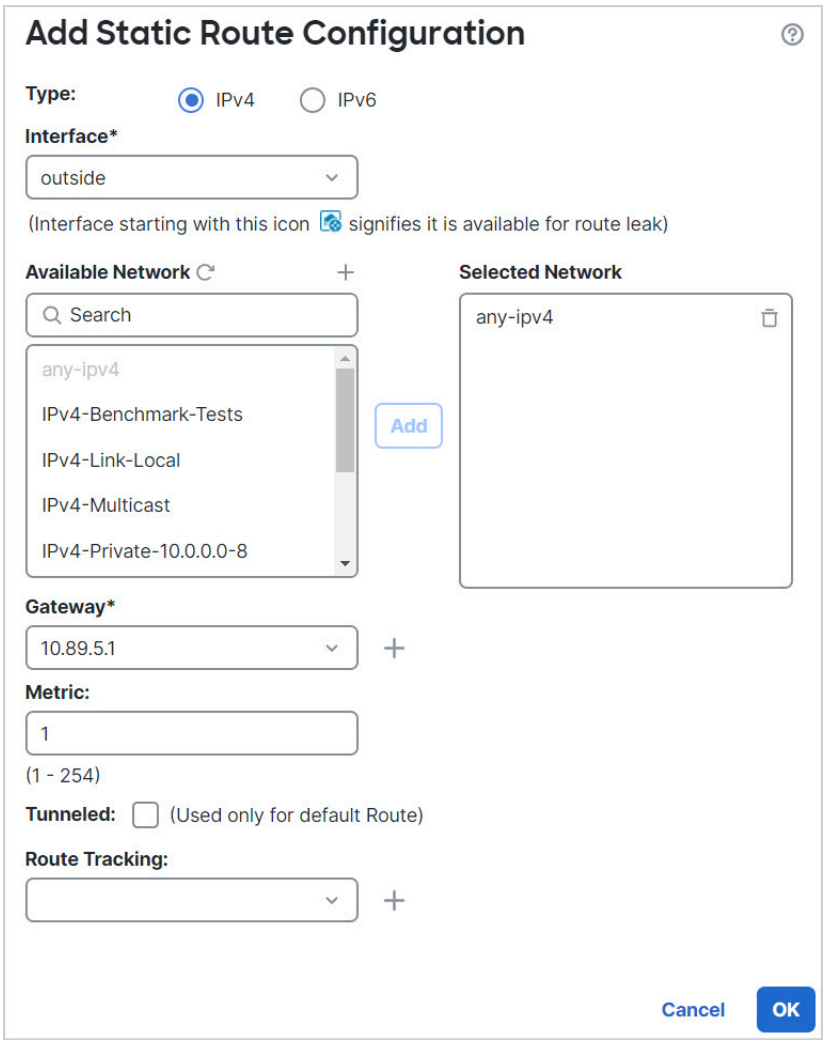


f) 点击**确定 (OK)**，然后点击**保存 (Save)**。

步骤 5 为两个接口添加等价默认静态路由，并在两个接口上启用 SLA 跟踪。

除网关外，路由应完全相同，并且都应具有指标 1。主接口应已具有您可以编辑的默认路由。

图 *31:* 添加/编辑静态路由



a) 点击**静态路由 (Static Route)**。
b) 点击**添加路由 (Add Route)** 以添加新路由，或点击现有路由的 **编辑** ()。
c) 从**接口 (Interface)** 下拉列表中选择接口。
d) 对于目标网络，从**可用网络 (Available Networks)** 框中选择 **any-ipv4**，然后点击**添加 (Add)**。
e) 输入默认**网关**。
f) 对于**路由跟踪 (Route Tracking)**，请点击 **添加** () 以添加新的 SLA 监控器对象。
g) 输入以下必需参数：

- 作为 防火墙管理中心 IP 地址的**监控地址**。
- **可用区域 (Available Zones)** 中的主要或辅助管理接口的区域；例如，为主接口对象选择外部区域，为辅助接口对象选择管理区域。

有关详细信息，请参阅SLA 监控器。

图 *32:* 添加 ***SLA*** 监控

h) 点击**保存 (Save)**，然后在**路由跟踪 (Route Tracking)** 下拉列表中选择您刚创建的 SLA 对象。
i) 点击**确定 (OK)**，然后点击**保存 (Save)**。
j) 对另一个管理接口的默认路由重复此操作。

步骤 6 部署配置更改；请参阅 部署配置更改。

作为此功能部署的一部分，防火墙管理中心 会为管理流量启用辅助接口，包括用于管理流量的自动生成的策略型路由配置，以到达正确的数据接口。防火墙管理中心 还会部署 **configure network management-data-interface** 命令的第二个实例。请注意，如果在 CLI 中编辑辅助接口，您将无法配置网关或以其他方式更改默认路由，因为只能在 防火墙管理中心 中编辑此接口的静态路由。

更改管理器访问接口设置

在设备或防火墙管理中心上更改任何管理器接口设置都可能中断管理连接。请参阅以下场景，了解如何更改接口设置并重新建立管理连接。

更改设备 IP 地址

更改设备 IP地址，然后在防火墙管理中心中更新地址。

设置设备 IP 地址

使用以下方法之一设置管理器访问接口 IP 地址。

在 *CLI* 中修改 *Firewall Threat Defense* 管理接口

使用 CLI 修改托管设备上的管理接口设置。这些设置中有许多是您在执行初始设置时设置的；此过程允许您更改这些设置，并设置其他设置，例如，启用事件接口（如果您的型号支持）或添加静态路由。

注释 本主题适用于专用管理接口。您也可以为管理配置数据接口。如果要更改该接口的网络设置，则应在 防火墙管理中心 中而不是在CLI中执行此操作。如果您需要对中断的管理连接进行故障排除，并且需要直接在 Firewall Threat Defense 上进行更改，请参阅 修改 CLI 中用于管理的 Firewall Threat Defense 数据接口 ， 第 39 页。

有关 Firewall Threat Defense CLI 的信息，请参阅*Cisco Secure Firewall Threat Defense 命令参考*。

注释 使用 SSH 时，在对管理接口进行更改时要小心；如果由于配置错误而无法重新连接，您将需要访问设备控制台端口。

注释 如果更改设备管理 IP 地址，请参阅以下有关 防火墙管理中心 连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add** 命令识别 防火墙管理中心 的方式（请参阅 向新的管理中心注册）：

- **IP 地址—无操作**。如果您使用可访问的IP地址识别 防火墙管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改 防火墙管理中心 中显示的设备 IP 地址，以保持信息同步；请参阅 更新防火墙管理中心中的主机名或 IP 地址，第 44 页。此操作有助于更快地重新建立连接。**注意**：如果您指定了无法访问的 防火墙管理中心 IP 地址，请参阅下面的 NAT ID 程序。
- **仅限 NAT ID-手动重新建立连接**。如果仅使用 NAT ID 识别 防火墙管理中心，则无法自动重新建立连接。在这种情况下，请根据 更新防火墙管理中心中的主机名或 IP 地址，第 44 页 更改 防火墙管理中心 中的设备管理 IP 地址。

注释 在高可用性配置中，当您从设备 CLI 或 防火墙管理中心修改已注册设备的管理 IP 地址时，即使在 HA 同步后，辅助 防火墙管理中心 也不会反映更改。要确保辅助 防火墙管理中心 也更新，请在两个之间切换角色，使辅助 成为主用设备。防火墙管理中心防火墙管理中心, 在备用的 **设备管理** 页面上修改已注册设备的管理IP地址防火墙管理中心。

开始之前

- 您可以使用 **configure user add** 命令创建可登录到 CLI 的用户账号；请参阅 在 CLI 中添加内部用户。您还可以根据外部身份验证配置 AAA 用户。

过程

步骤 1 通过控制台端口或使用 SSH 连接至设备 CLI。

请参阅登录到设备的命令行界面。

步骤 2 使用管理员用户名和密码登录。

步骤 3 (仅限 Firepower 4100/9300/Secure Firewall 4200/6100）将第二个管理接口启用为仅事件接口。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

您始终需要用于管理通信的管理接口。如果您的设备有第二个管理接口，则可以为仅事件流量启用该接口。

您可以选择使用 **configure network management-interface disable-events-channel** 命令禁用主管理接口的事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件通道，设备也会通过管理接口发送事件。

无法同时禁用接口上的事件通道和管理通道。

要使用单独的事件接口，您必须在专用于事件流量的防火墙管理中心上启用一个事件专用接口。请参阅*Cisco Secure Firewall Management Center* 管理指南。

示例：

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

步骤 4 配置管理接口和/或事件接口的 IP 地址：

如果未指定 *management_interface* 参数，则更改默认管理接口的网络设置。配置事件接口时，请确保指定 *management_interface* 参数。事件接口可以与管理接口位于不同的网络中，也可以位于同一网络中。如果连接到您正在配置的接口，您将断开连接。您可以重新连接到新 IP 地址。

a) 配置 IPv4 地址：

- 手动配置：

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  请注意，此命令中的 门户*_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 门户*_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您设置 门户*_ip* 以用于管理接口，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

  示例：

  ```
  > configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
  Setting IPv4 network configuration.
  Network settings changed.

  >
  ```

- DHCP（只有默认的管理接口上才支持）：

  configure network ipv4 dhcp

b) 配置 IPv6 地址：

- 无状态自动配置：

  configure network ipv6 router [*management_interface*]

  示例：

  ```
  > configure network ipv6 router management0
  Setting IPv6 network configuration.
  Network settings changed.
  ```

```
>
```

- 手动配置：

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  请注意，此命令中的 *ipv6_gateway_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *ipv6_gateway_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *ipv6_gateway_ip* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

  示例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6（只有默认的管理接口上才支持）：

  configure network ipv6 dhcp

步骤 5 对于IPv6，启用或禁用ICMPv6回应应答和目的地不可达消息。默认情况下，系统会启用这些消息。

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。

示例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

步骤 6 在默认管理接口上启用 DHCP 服务器，以便向已连接的主机提供 IP 地址：

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

示例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

只有手动设置管理接口 IP 地址时，才能配置 DHCP 服务器。Firewall Management Center Virtual上不支持此命令。要显示 DHCP 服务器的状态，请输入 **show network-dhcp-server**：

```
> show network-dhcp-server
```

```
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

步骤 7 如果 防火墙管理中心位于远程网络上，则将为仅事件接口添加静态路由；否则，所有流量都将通过管理接口与默认路由匹配。

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

对于 默认 路由，请勿使用此命令；当您使用 **configure network ipv4** 或 **ipv6** 命令时，只能更改默认路由网关 IP 地址（请参阅步骤 步骤 4，第 35 页）。

示例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

要显示静态路由，请输入 **show network-static-routes**（不显示默认路由）：

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

步骤 8 设置主机名：

configure network hostname *name*

示例：

```
> configure network hostname farscape1.cisco.com
```

在重新启动之后，系统日志消息不会反映新的主机名。

步骤 9 选择搜索域：

configure network dns searchdomains *domain_list*

示例：

```
> configure network dns searchdomains example.com,cisco.com
```

为设备设置搜索域，用逗号隔开。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

步骤 10 设置多达 3 个 DNS 服务器，用逗号隔开：

configure network dns servers *dns_ip_list*

示例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

步骤 11 设置与 防火墙管理中心通信的远程管理端口：

configure network management-interface tcpport *number*

示例：

```
> configure network management-interface tcpport 8555
```

防火墙管理中心和托管设备使用双向、TLS-1.3 加密的通信通道（默认情况下在端口 8305 上）进行通信。使用多实例模式时，请勿更改管理端口；仅支持 8305 端口。

注释
思科强烈建议保留远程管理端口的默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。

步骤 12 （仅限 Firewall Threat Defense）设置管理或事件接口 MTU。默认 MTU 为 1500 字节。

configure network mtu [字节] [*interface_id*]

- 字节-设置 MTU（以字节为单位）。对于管理接口，如果启用 IPv4，则值可以介于 64 和 1500 之间；如果启用 IPv6，则值可以介于 1280 和 1500 之间。对于事件接口，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入 字节，系统会提示您输入值。
- *interface_id*-指定要设置 MTU 的接口 ID。使用 **show network** 命令查看可用的接口 ID，例如 management0、management1、br1 和 eth0，具体取决于平台。如果未指定接口，则使用管理接口。

示例：

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

步骤 13 配置 HTTP 代理。该设备配置为直接连接到互联网上的端口 TCP/443 (HTTPS) 和 TCP/80 (HTTP)。您可以通过 HTTP 摘要对代理服务器进行身份验证。发出命令后，系统将提示您 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

注释
对于 Firewall Threat Defense 上的代理密码，只能使用 A-Z、a-z 和 0-9 字符。

configure network http-proxy

示例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

步骤 14 如果更改设备管理 IP 地址，请参阅以下有关 防火墙管理中心 连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add** 命令识别 防火墙管理中心 的方式（请参阅 向新的管理中心注册）：

- **IP 地址—无操作**。如果您使用可访问的IP地址识别 防火墙管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改 防火墙管理中心 中显示的设备 IP 地址，以保持信息同步；请参阅 更新防火墙管理中心中的主机名或 IP 地址，第 44 页。此操作有助于更快地重新建立连接。**注意**：如果指定了无法访问的 防火墙管理中心 IP 地址，则必须使用 更新防火墙管理中心中的主机名或 IP 地址，第 44 页 手动重新建立连接。
- **仅限 NAT ID-手动重新建立连接**。如果仅使用 NAT ID 识别 防火墙管理中心，则无法自动重新建立连接。在这种情况下，请根据 更新防火墙管理中心中的主机名或 IP 地址，第 44 页 更改 防火墙管理中心 中的设备管理 IP 地址。

修改 *CLI* 中用于管理的 *Firewall Threat Defense* 数据接口

如果 Firewall Threat Defense 和 防火墙管理中心 之间的管理连接中断，并且您希望指定新的数据接口来替换旧接口，请使用 Firewall Threat Defense CLI 配置新接口。

如果管理连接处于活动状态，则应使用 防火墙管理中心 对现有数据接口进行任何更改（参见修改 GUI 中用于管理的 Firewall Threat Defense 数据接口，第 42 页）。有关数据管理接口的初始设置，请参阅使用 CLI 完成Firewall Threat Defense初始配置中的 **configure network management-data-interface** 命令。

对于高可用性对，在两台设备上执行所有 CLI 步骤。在 防火墙管理中心中，仅对主用设备执行以下步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

注释 本主题适用于为管理配置的数据接口，而不是专用的管理接口。如果要更改管理接口的网络设置，请参阅 在 CLI 中修改 Firewall Threat Defense 管理接口，第 33 页。

有关 Firewall Threat Defense CLI 的信息，请参阅*Cisco Secure Firewall Threat Defense* 命令参考。

过程

步骤 1 如果要将数据管理接口更改为新接口，请将当前接口电缆移至新接口。

步骤 2 连接到设备 CLI。

使用这些命令时，应使用控制台端口。如果您正在执行初始设置，则可能会断开与管理接口的连接。如果由于管理连接中断而正在编辑配置，并且您具有专用管理接口的 SSH 访问权限，则可以使用该 SSH 连接。

请参阅登录到设备的命令行界面。

步骤 3 使用**管理员**用户名和密码登录。

步骤 4 禁用接口，以便您重新配置其设置。

configure network management-data-interface disable

注释
如果您只想在同一接口上设置新的 IPv4 地址而不进行任何其他更改，则可以跳过此步骤。其他更改要求您首先禁用该接口。

示例：

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a gateway
 on management interface using the command 'configure network'
```

步骤 5 配置用于管理器访问的新数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

当您将数据管理接口更改为同一网络上的新接口时，请使用与上一个接口相同的设置（接口 ID 除外）。此外，对于 **是否希望在应用之前清除所有设备配置？(y/n) [n]:** 选项，选择 **y**。此选项将清除旧的数据管理接口配置，以便您可以成功地在新接口上重新使用IP地址和接口名称。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 6 （可选） 限制在特定网络上通过数据接口访问 防火墙管理中心。

configure network management-data-interface client *ip_address netmask*

默认情况下，允许所有网络。

步骤 7 更新防火墙管理中心中的主机名或 IP 地址，第 44 页。

连接将自动重新建立，但在防火墙管理中心中禁用和重新启用连接将有助于更快地重新建立连接。或者，您可能需要根据链接的程序更新 防火墙管理中心 中的设备 IP 地址。

步骤 8 检查管理连接是否已重新建立。

sftunnel-status-brief

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

步骤 9 在 防火墙管理中心中，选择 **设备** > **设备管理**，然后点击 **编辑** ()。**在 设备 管理区域中，点击 刷新**。

防火墙管理中心 检测接口和默认路由配置更改，并阻止部署到。当您在设备上本地更改数据接口设置时，必须在 防火墙管理中心 中手动协调这些更改。您可以在**配置 (Configuration)** 选项卡上查看 防火墙管理中心 和 之间的差异。

步骤 10 选择**接口**并进行以下更改。

a) 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的管理器访问。

b) 使用旧接口（在 CLI 中使用的接口）的配置配置新的数据管理接口，并为其启用管理器访问。

步骤 11 点击**路由**选项卡，点击 **静态路由**，然后将默认路由从旧数据管理界面更改为新界面。

步骤 12 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

下次部署时，防火墙管理中心 配置将覆盖 Firewall Threat Defense 上任何剩余的冲突设置。在您重新部署之前，您有责任在 防火墙管理中心 中手动修复配置。

您将看到“配置已清除”(Config was cleared) 和“管理器 访问已更改并确认 (Manager/FMC access changed and acknowledged)”的预期消息。

修改 *GUI* 中用于管理的 *Firewall Threat Defense* 数据接口

如果管理连接启动，但要更改用于管理器访问的数据接口的 IP 地址，请执行以下步骤。例如，如果使用 零接触调配注册设备，则需要先将 IP 地址更改为静态地址，然后才能启用高可用性。

您也可以在 CLI 中更改接口设置，但我们建议仅在管理连接断开时使用该方法。无论如何，您在 CLI 中所做的任何更改都必须在 GUI 中复制。

过程

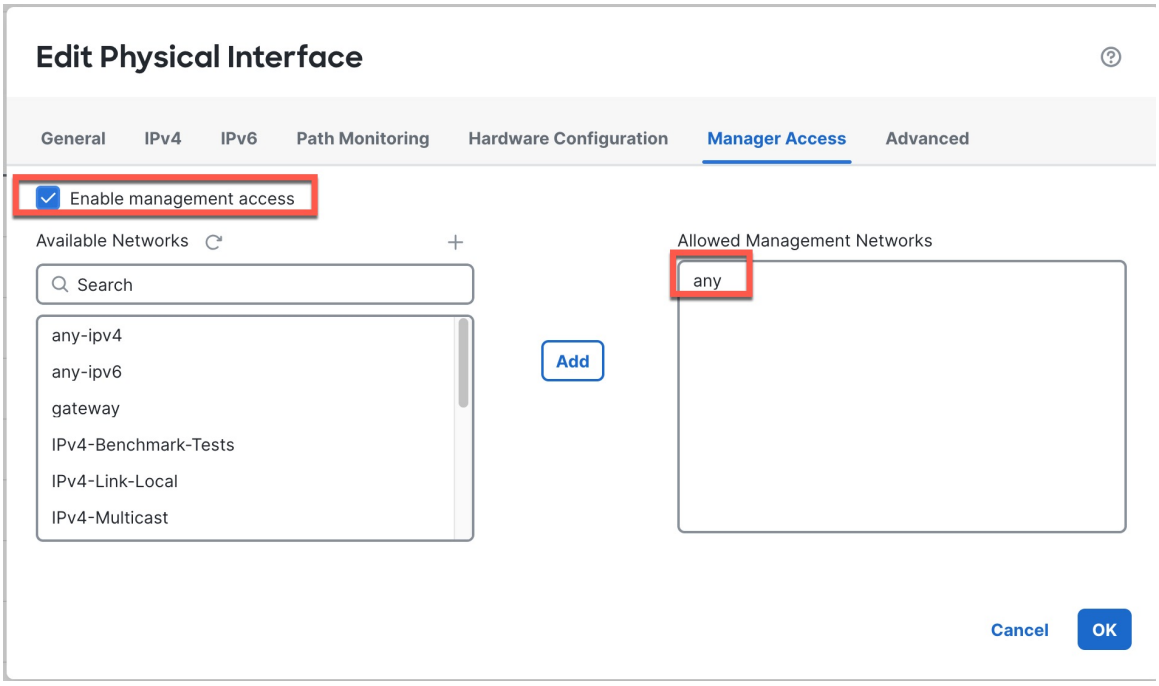
步骤 1 选择 **设备** > **设备管理**，然后点击设备旁边的 **编辑** (✎) 。

步骤 2 选择**接口**。

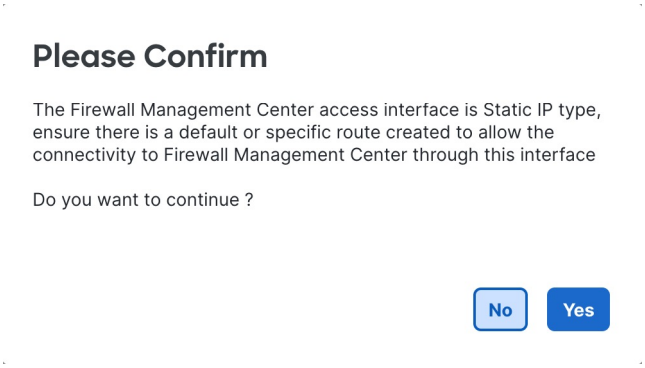
步骤 3 如果要更改用于管理器访问的接口，请执行以下操作：

a) 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的管理器访问。

b) 使用旧接口的配置配置新的数据管理接口，并为其启用管理器访问。



c) 如果使用静态 IP 地址，系统会提醒您确保具有默认路由。点击**是 (Yes)**。



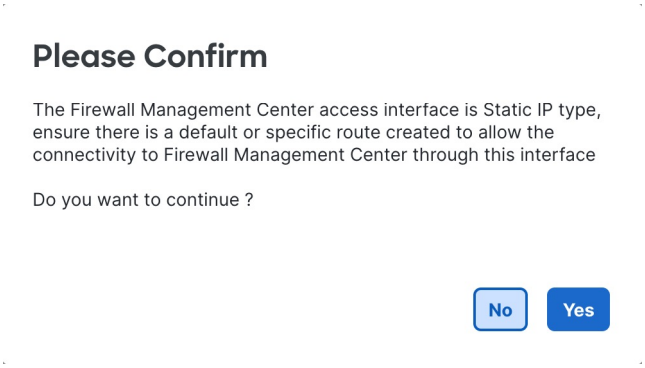
d) 点击 **确定** 退出该界面。

e) 在**接口 (Interfaces)** 页面上点击**保存 (Save)**。

步骤 4 如果只想更改 IP 地址：

a) 请更改 IP 地址。

b) 对于静态 IP 地址，建议您确保具有默认路由。点击**是 (Yes)**。



c) 点击 **确定** 退出该界面。

d) 在**接口 (Interfaces)** 页面上点击**保存 (Save)**。

步骤 5 点击 **路由** 选项卡，点击 **静态路由**，然后添加或更改管理访问接口的默认或静态路由。

步骤 6 部署配置更改；请参阅 部署配置更改。

防火墙管理中心将通过当前连接部署配置更改。在部署后，数据接口将具有新的IP地址，因此需要重新建立管理连接。

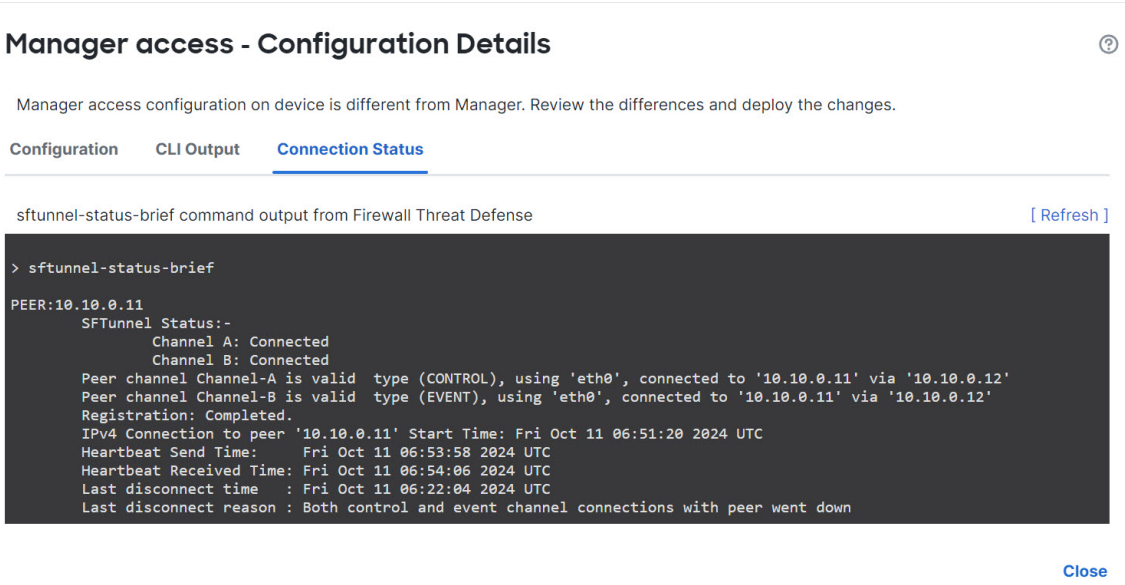
步骤 7 更新防火墙管理中心中的主机名或 IP 地址，第 44 页。

步骤 8 确保管理连接已重新建立。

在**设备** 区域中，在**管理** 字段中，点击 **管理器访问详细信息：配**，然后点击 **连接状态**。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *33:* 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 64 页。

更新防火墙管理中心中的主机名或 IP 地址

如果您在将设备的主机名或 IP 地址添加到 防火墙管理中心 后，对其进行编辑（例如使用设备的 CLI），可能需要使用以下操作步骤手动更新管理 防火墙管理中心 上的主机名或 IP 地址。

更改设备管理 IP 地址的步骤，请参阅 在 CLI 中修改 Firewall Threat Defense 管理接口，第 33 页。

如果您在注册设备时仅使用了 NAT ID，则该 IP 在此页面上显示为 **NO-IP**，您无需更新 IP 地址/主机名。

如果您使用零接触调配在外部接口上注册设备，则会自动生成主机名以及匹配的 DDNS 配置；在这种情况下，您无法编辑主机名。

过程

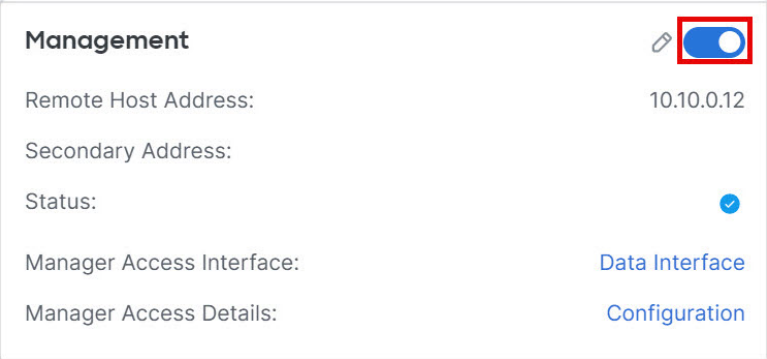
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要修改管理选项的设备旁边，点击 **编辑** ()。

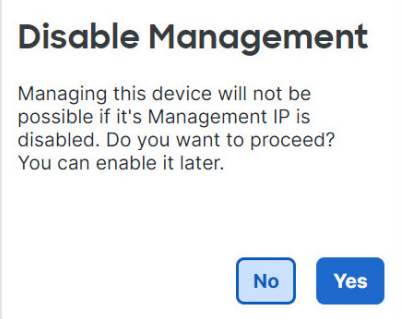
步骤 3 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

步骤 4 点击滑块暂时禁用管理，使其处于禁用状态 **滑块已禁用** ()。

图 *34:* 禁用管理



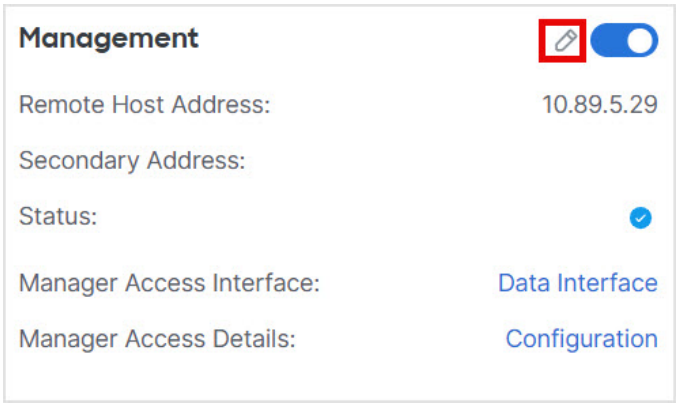
系统将提示您继续禁用管理；点击 **是**。



禁用管理会阻止 防火墙管理中心 和设备之间的连接，但**不会**从 防火墙管理中心 取消注册设备。

步骤 5 通过点击 **编辑** (✎) 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

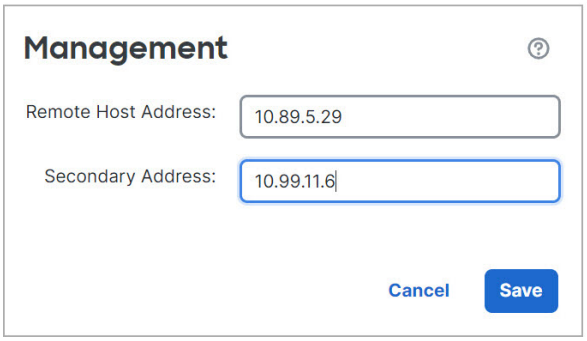
图 *35:* 编辑管理地址



步骤 6 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存**。

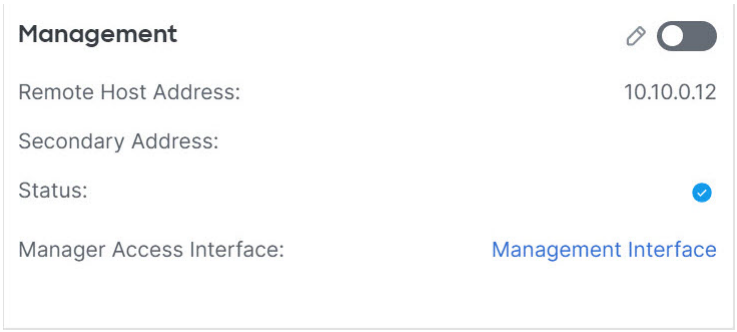
有关使用辅助管理器访问数据接口的信息，请参阅配置冗余管理器访问数据接口，第 28 页。

图 *36:* 管理 *IP* 地址



步骤 7 点击滑块重新启用管理，使其处于启用状态 **滑块已启用** ( )。

图 *37:* 启用管理连接



更改 防火墙管理中心 IP 地址

如果更改 防火墙管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的防火墙管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到防火墙管理中心 并指定仅NAT ID。即使在其他情况下，我们也建议保持防火墙管理中心IP地址或主机名为最新状态，以实现额外的网络恢复能力。

过程

步骤 1 请更改 防火墙管理中心 IP 地址。

注意
对所连接的防火墙管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 防火墙管理中心 控制台端口以重新配置Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择**管理** > **配置** > **管理接口**。

b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存**。

步骤 2 在 Firewall Threat Defense CLI 中，查看 防火墙管理中心 标识符。

show managers

示例：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

步骤 3 在 Firewall Threat Defense CLI 中，编辑 防火墙管理中心 IP 地址或主机名。

configure manager edit 标识符 {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

如果 防火墙管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

管理连接将关闭，然后重新建立。您可以使用 **sftunnel-status** 命令监控连接状态。

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

更改防火墙管理中心和威胁防御 IP 地址

如果需要将 防火墙管理中心 和 Firewall Threat Defense IP 地址移至新网络，则可能需要同时更改这些地址。

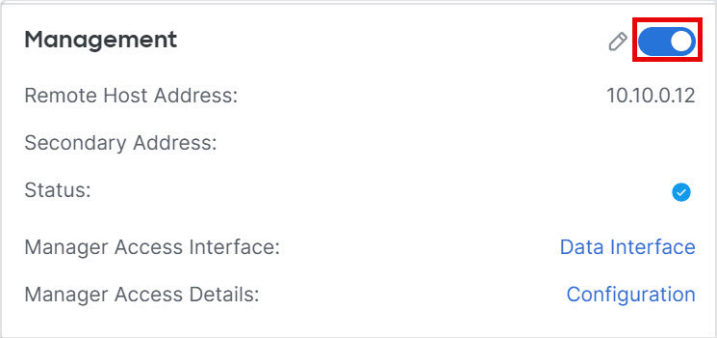
过程

步骤 1 禁用管理连接。

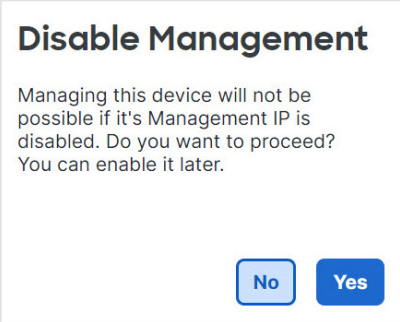
对于高可用性对或集群，在所有设备上执行这些步骤。

a) 选择**设备** > **设备管理**。
b) 点击设备旁边的 **编辑** ()。
c) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。
d) 点击滑块暂时禁用管理，使其处于禁用状态 ()。

图 *38:* 禁用管理



系统将提示您继续禁用管理；点击 **是**。



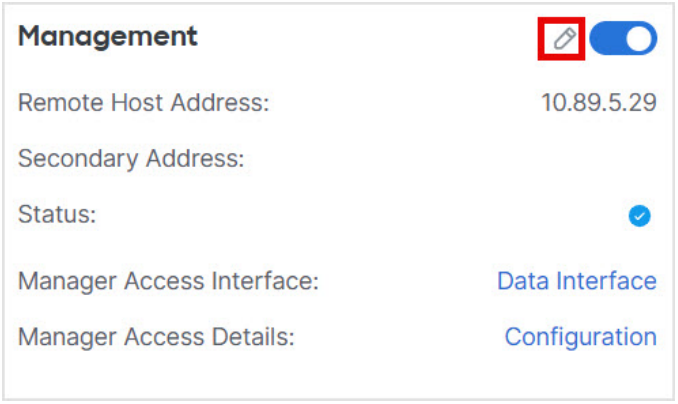
步骤 2 将 防火墙管理中心 中的设备 IP 地址更改为新的设备 IP 地址。

稍后您将更改设备上的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

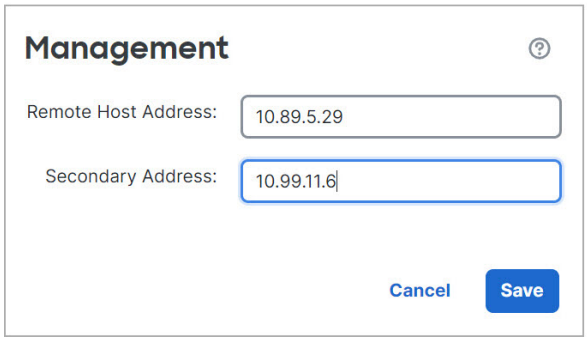
a) 通过点击 **编辑** (✎) 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

图 *39:* 编辑管理地址



b) 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存**。

图 *40:* 管理 *IP* 地址



步骤 3 请更改 防火墙管理中心 IP 地址。

注意
对所连接的防火墙管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 防火墙管理中心 控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择**管理** > **配置** > **管理接口**。
b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存**。

步骤 4 更改设备上的管理器 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 在 Firewall Threat Defense CLI 中，查看 防火墙管理中心 标识符。

show managers

示例：

```
> show managers
Type                       : Manager
Host                       : 10.10.1.4
Display name               : 10.10.1.4
Identifier                 : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration               : Completed
Management type            : Configuration
```

b) 编辑 防火墙管理中心 IP 地址或主机名。

configure manager edit 标识符 {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

如果 防火墙管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

示例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

步骤 5 在控制台端口更改管理器访问接口的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

如果您使用专用管理接口：

configure network ipv4

configure network ipv6

如果您使用专用管理接口：

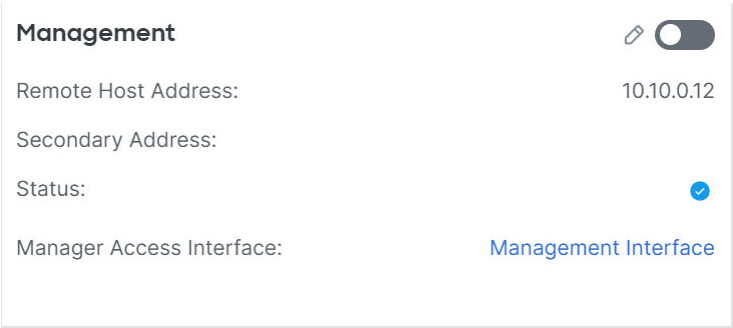
configure network management-data-interface disable

configure network management-data-interface

步骤 6 点击滑块重新启用管理，使其处于启用状态 ( )。

对于高可用性对或集群，在所有设备上执行这些步骤。

图 *41:* 启用管理连接



步骤 7 （如果使用数据接口进行管理器访问）刷新 防火墙管理中心中的数据接口设置。

对于高可用性对，请在两台设备上执行此步骤。

a) 选择**设备** > **设备管理**，点击**管理器访问 - 配置详细信息**，然后点击**刷新**。
b) 选择**设备** > **设备管理**，点击**接口**选项卡，然后设置 IP 地址以便与新地址匹配。
c) 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

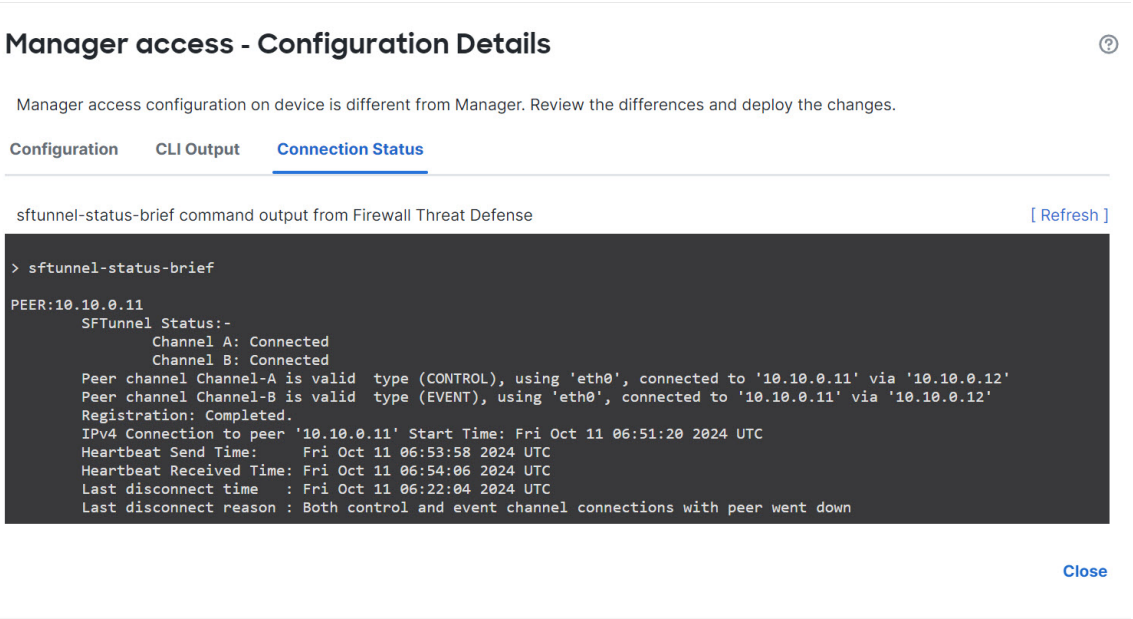
步骤 8 确保管理连接已重新建立。

在防火墙管理中心中，检查管理连接状态。导航到 **设备** > **设备管理**，然后点击**设备**选项卡下的**管理**部分。然后点击**管理器访问 - 配置详细信息**以查看**连接状态**页面。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *42:* 连接状态



步骤 9 （对于高可用性 防火墙管理中心 对）在辅助 防火墙管理中心上重复配置更改。

a) 更改辅助 防火墙管理中心 IP 地址。
b) 在两台设备上指定新的对等地址。
c) 将辅助设备设置为主用设备。
d) 禁用设备管理连接。
e) 更改 防火墙管理中心 中的设备 IP 地址。
f) 重新启用管理连接。

更改管理器访问接口

注册设备后，可以在管理接口和数据接口之间更改管理器访问接口。

将管理器访问接口从管理更改为数据

你可以从专门的管理界面，或从数据界面管理 Firewall Threat Defense。如果要在添加设备转至 防火墙管理中心 后更改管理器访问接口，请按照以下步骤从管理接口迁移到数据接口。要迁移另一个方向，请参阅将管理器访问接口从数据更改为管理，第 56 页。

启动从管理到数据的管理器访问迁移会导致 防火墙管理中心 在部署到 Firewall Threat Defense 时应用阻止。要删除数据块，请在数据接口上启用管理器访问。

请参阅以下步骤以启用数据接口上的管理器访问，并配置其他所需的设置。

开始之前

对于高可用性对，除非另有说明，否则请仅在主用设备上执行所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

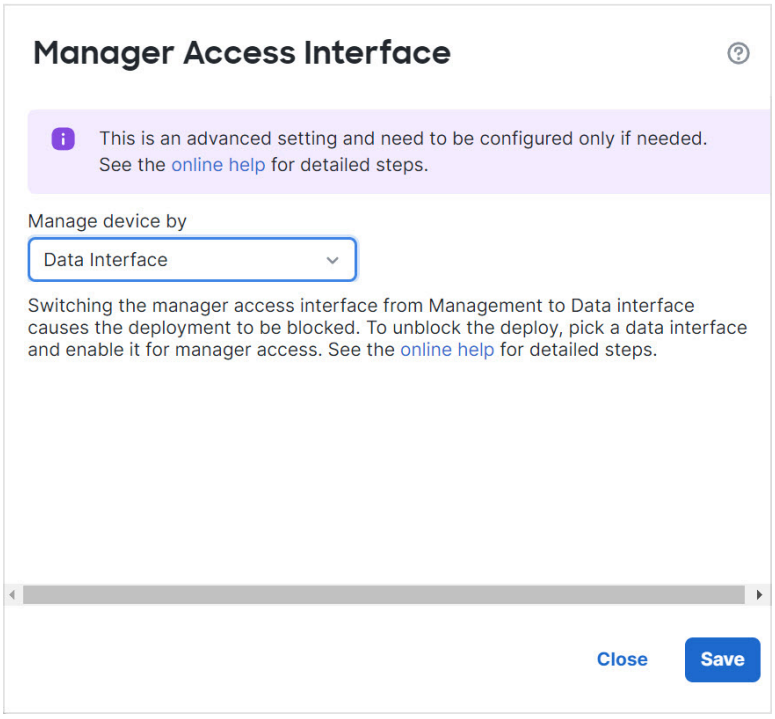
过程

步骤 1 初始化接口迁移。

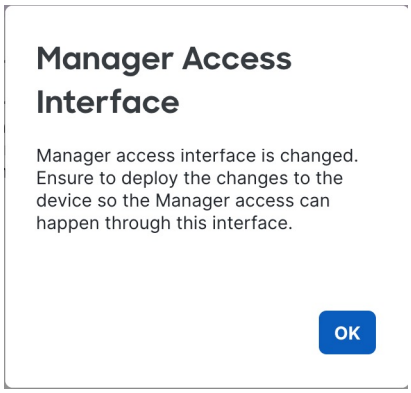
a) 在 设备设备管理 页面，然后点击设备的 **设备** > **设备管理** 。**编辑** ( )**点击 设备**，然后在**管理**区域中点击FMC 访问接口的链接。

管理器访问接口 (Manager Access Interface) 字段会显示当前管理接口。当您点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型 **数据接口**。

图 *43:* 管理器访问接口

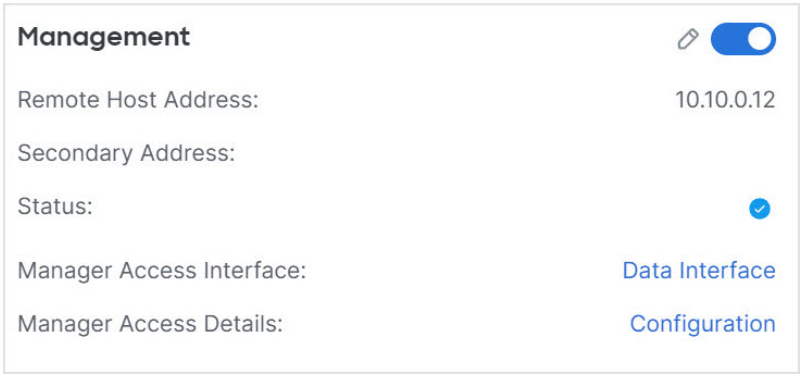


b) 点击 **确定** ，然后点击 **关闭 (Close)**。



您现在必须完成此程序中的其余步骤，才能在数据接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：数据接口 (Manager Access Interface: Data Interface)** 以及**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

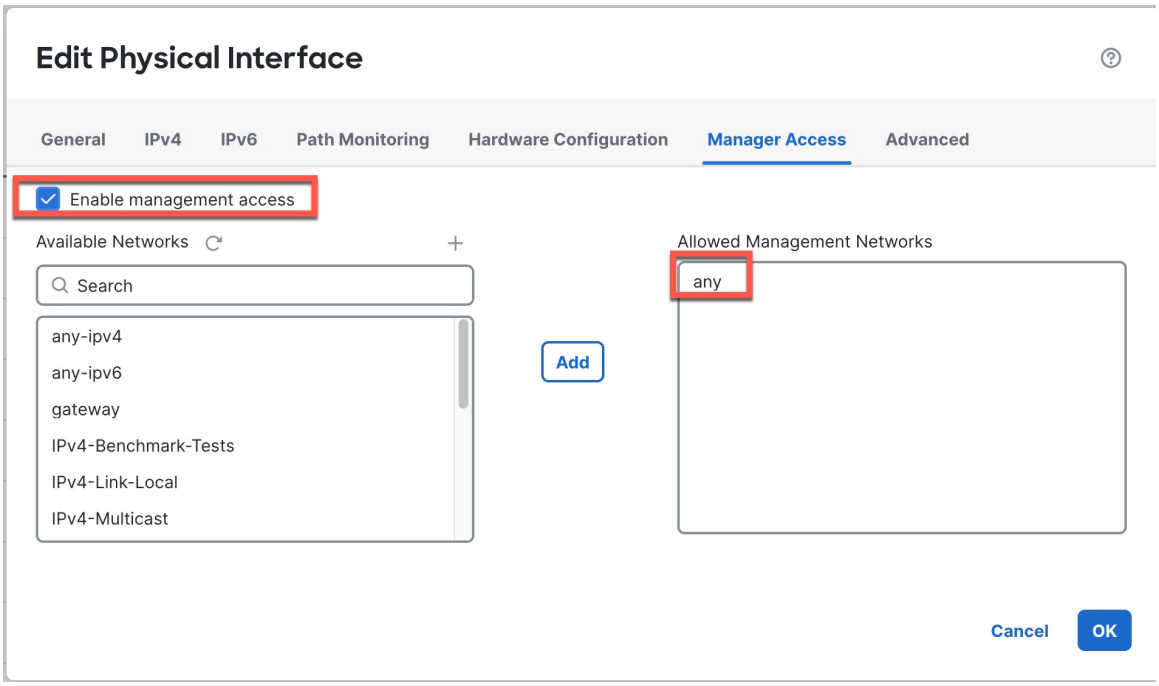
图 *44:* 管理器访问



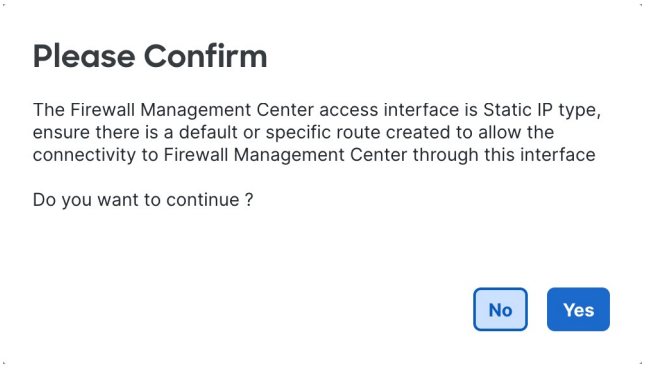
如果点击**配置 (Configuration)**，将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 将显示“等待部署” (Deploy pending) 状态。

步骤 2 在数据接口上启用管理器访问。点击**接口 (Interfaces)**，点击接口的**编辑** (✎)，然后点击**管理器访问 (Manager Access**。

选中**启用管理访问 (Enable management access)**，然后点击**确定**。默认情况下，系统允许所有网络，但您可以在允许 防火墙管理中心 地址的情况下限制访问。



如果管理器访问接口使用静态 IP 地址，系统会提醒您为其配置路由。



在**接口 (Interfaces)**页面上点击**保存**。有关接口设置的详细信息，请参阅配置路由模式接口。您可在一个数据接口以及一个可选的辅助接口上启用管理器访问。确保这些接口使用名称和 IP 地址进行了充分配置，并且已启用。

如果使用辅助接口实现冗余，请参阅配置冗余管理器访问数据接口，第 28 页以了解其他所需的配置。

步骤 3 （可选） 如果对接口使用DHCP，请在 **设备** 设备管理DHCPDDNS 页面上启用 Web 类型 DDNS 方法。导航至 **设备** > **设备管理**，然后点击 **DHCP** 选项卡下的 **DDNS** 。

请参阅配置动态 DNS。如果 FTD 的 IP 地址发生变化，DDNS 可确保 防火墙管理中心 接通完全限定域名 (FQDN) 内的 Firewall Threat Defense。

步骤 4 确保 Firewall Threat Defense 可以通过数据接口路由到防火墙管理中心；如果需要，在 设备 (Devices) 设备管理 (Device Management)路由 (Routing)静态路由 (Routing)上添加静态路由。导航至 **设备** > **设备管理** ，然后点击 **“路由”(Routing)** 选项卡下的 **静态路由 (Static Route)** 。

请参阅添加静态路由。

步骤 5 （可选） 在平台设置策略中配置 DNS：选择 **设备** > **平台设置**，然后点击 **DNS**。将此策略应用到此设备。

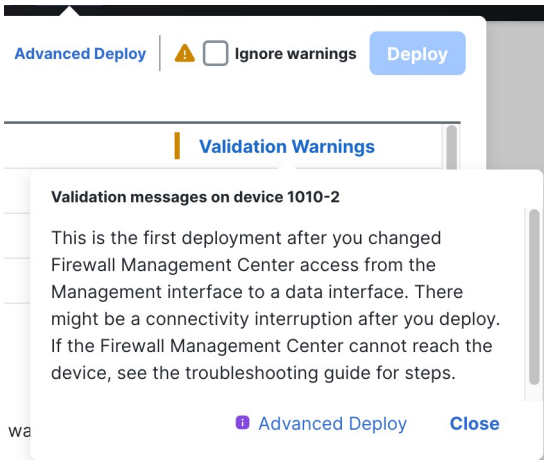
请参阅DNS。如果使用 DDNS，则需要 DNS。您也可以将 DNS 用于安全策略中的 FQDN。

步骤 6 （可选） 在平台设置策略中为数据接口启用 SSH，并通过**设备** > **设备管理**页面将其应用于此设备。点击设备的 **编辑** ()，然后点击 **SSH 访问 (SSH Access)**。

请参阅SSH 访问。默认情况下，数据接口上未启用 SSH，因此，如果要使用 SSH 管理 Firewall Threat Defense，则需要明确允许它。

步骤 7 部署配置更改；请参阅 部署配置更改。

您将看到一条验证错误，要求您确认更改是否更改了管理器访问接口。选中**忽略警告 (Ignore warnings)** 并再次部署。



防火墙管理中心 将通过当前管理接口部署配置更改。部署后，数据接口现在可供使用，但与管理的原始管理连接仍处于活动状态。

步骤 8 在 Firewall Threat Defense CLI（最好从控制台端口），将管理接口设置为使用静态 IP 地址，并将网关设置为使用数据接口。 对于高可用性，请在两台设备上执行此步骤。

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask* - 虽然您不打算使用管理接口，但必须设置静态IP地址，例如专用地址，以便将网关设置为 **数据接口**（请参阅下一个项目符号）。您无法使用 DHCP，因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。
- **data-interfaces** - 此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。

我们建议您使用控制台端口而不是 SSH 连接，因为当您更改管理接口网络设置时，您的 SSH 会话将断开。

步骤 9 如有必要，请重新连接 Firewall Threat Defense，使其能够到达数据接口上的 防火墙管理中心。 对于高可用性，请在两台设备上执行此步骤。

步骤 10 在 防火墙管理中心 中，禁用管理连接，在设备管理区域的 **设备 设备管理** 设备中更新 Firewall Threat Defense 的**远程主机地址**IP 地址和可选**辅助地址**，然后重新启用连接。**设备 > 设备管理**

请参阅更新防火墙管理中心中的主机名或 IP 地址 ，第 44 页。如果在将 Firewall Threat Defense 添加到 防火墙管理中心 时使用了 Firewall Threat Defense 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

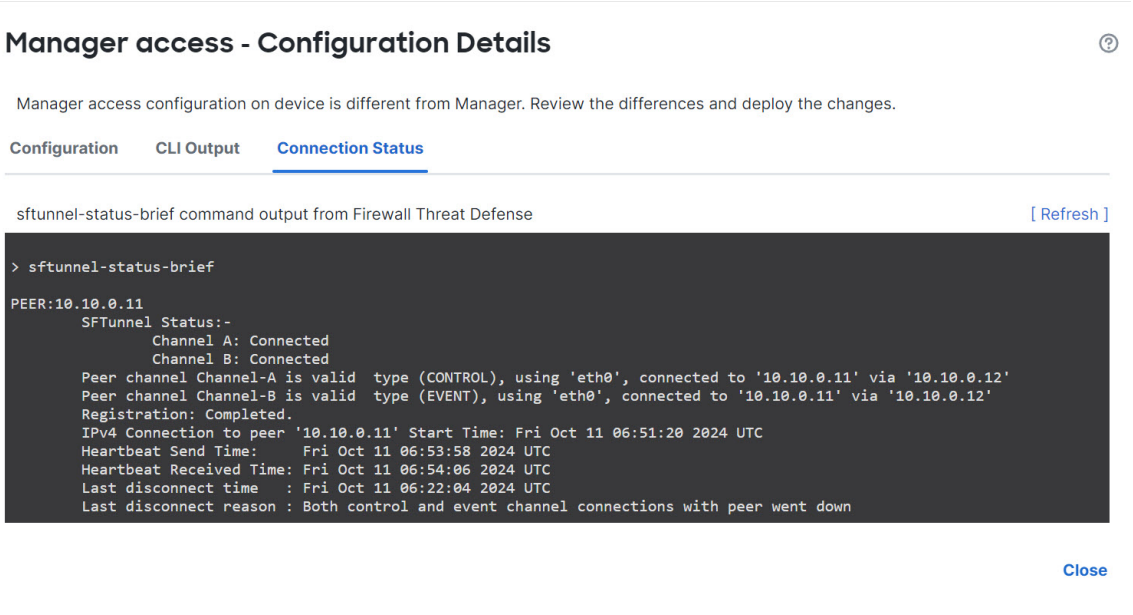
步骤 11 确保管理连接已重新建立。

在**设备 > 设备管理**页面，点击**管理器访问详细信息：配置 (Manager Access Details: Configuration)** 然后点击**连接状态 (Connection Status)**。

或者，您可以在 Firewall Threat Defense CLI 中进行检查。输入 **sftunnel-status-brief** 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *45:* 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 64 页。

将管理器访问接口从数据更改为管理

你可以从专门的管理界面，或从数据界面管理 Firewall Threat Defense。如果要在添加设备到 防火墙管理中心 后更改管理器访问接口，请按照以下步骤从数据接口迁移到管理接口。要迁移另一个方向，请参阅将管理器访问接口从管理更改为数据，第 51 页。

启动从数据到管理的管理器访问迁移会导致 防火墙管理中心 在部署到 Firewall Threat Defense 时应用阻止。您必须在数据接口上禁用管理器访问权限才能删除数据块。

请参阅以下步骤以禁用数据接口上的管理器访问，并配置其他所需的设置。

开始之前

对于高可用性对，除非另有说明，否则请仅在主用设备上执行所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

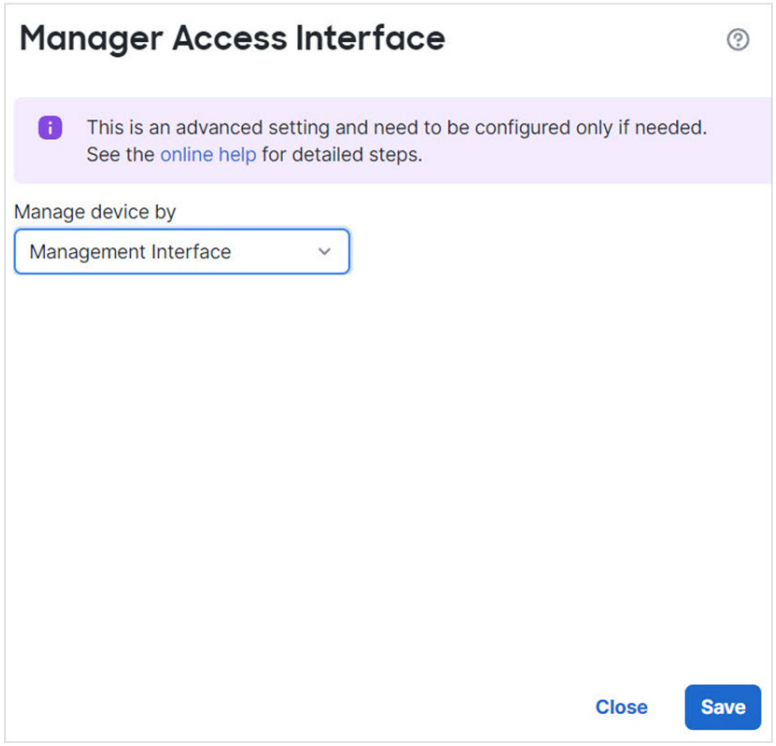
过程

步骤 1 初始化接口迁移。

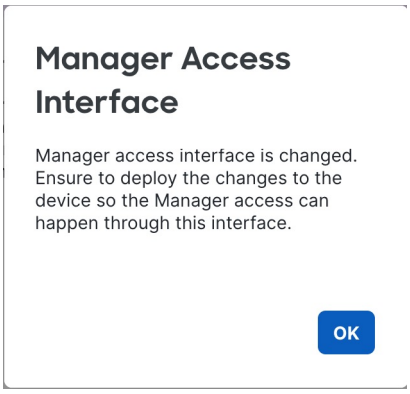
a) 在 设备设备管理 页面，然后点击设备的 **设备** > **设备管理** 。**编辑** (✎)**点击 设备**，然后在**管理**区域中点击FMC 访问接口的链接。

管理器访问接口 (Manager Access Interface) 字段会将当前管理接口显示为数据。点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型， **管理接口**。

图 ***46:*** 管理器访问接口



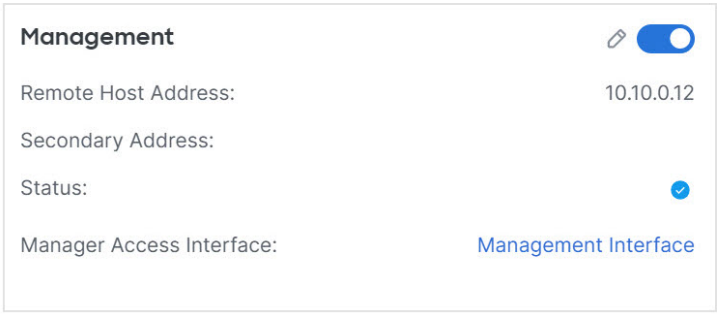
b) 点击**保存**。



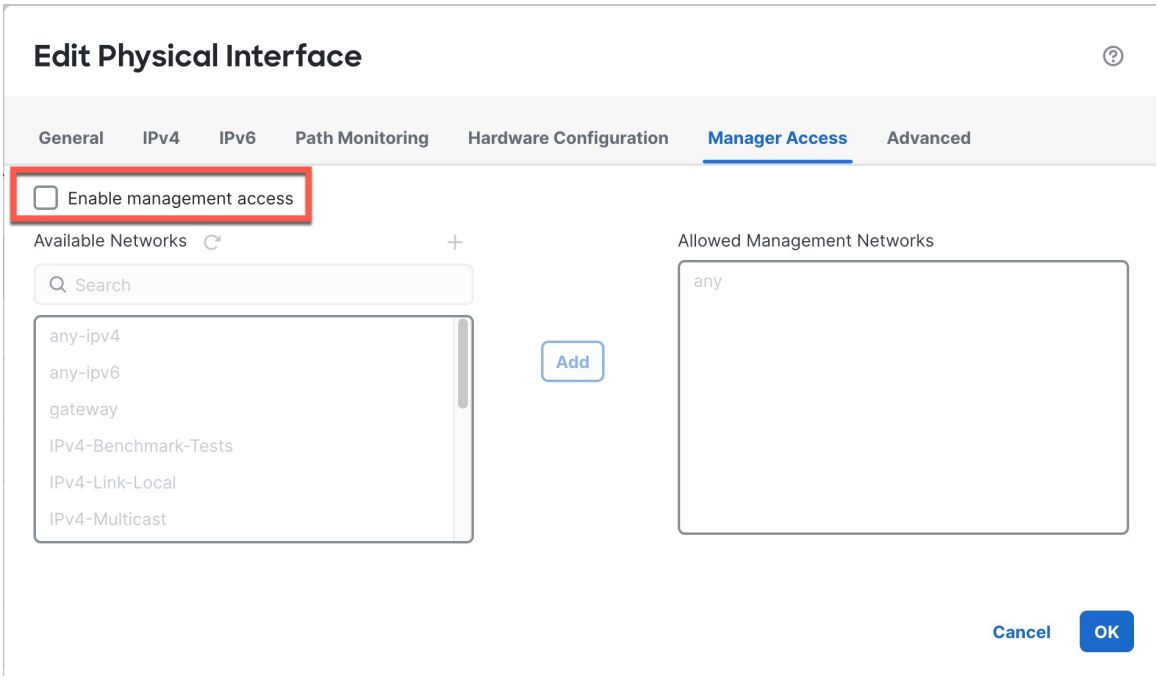
点击**确定**，然后点击**关闭 (Close)**。

您现在必须完成此程序中的其余步骤，才能在管理接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：管理接口 (Manager Access Interface: Management Interface)**。

图 *47:* 管理器访问



步骤 2 在数据接口上禁用管理器访问。点击 **接口 (Interfaces)**，点击接口所对应的 **编辑** (✎)，然后点击 **管理器访问 (Manager Access**。



取消选中**启用管理访问 (Enable management access)**，然后点击**确定**。在**接口 (Interfaces)** 页面上点击**保存**。此步骤将删除部署时的阻止。

步骤 3 如果尚未执行此操作，请在“平台设置”策略中为数据接口配置 DNS 设置，然后在 设备平台设置 DNS上将其应用至设备。**设备** > **设备管理**点击设备的 **编辑** (✎)，然后点击 **DNS**。

请参阅DNS。在数据接口上禁用管理器访问的 防火墙管理中心 部署将删除任何本地 DNS 配置。如果该 DNS 服务器用于任何安全策略，例如访问规则中的 FQDN，则必须使用 防火墙管理中心 重新应用 DNS 配置。

步骤 4 部署配置更改；请参阅 部署配置更改。

将 防火墙管理中心 通过当前数据接口部署配置更改。

步骤 5 如有必要，请重新连接 Firewall Threat Defense，以便它可以到达管理接口上的 防火墙管理中心。 对于高可用性，请在两台设备上执行此步骤。

步骤 6 在 Firewall Threat Defense CLI 中，使用静态 IP 地址或 DHCP 配置管理接口 IP 地址和网关。 对于高可用性，请在两台设备上执行此步骤。

当您最初配置用于管理器访问的数据接口时，管理网关设置为 data-interfaces，它通过背板转发管理流量，以便可以通过管理器访问数据接口路由。您现在需要为管理网络上的网关设置 IP 地址。

静态 IP 地址：

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP:

configure network{**ipv4** | **ipv6**} **dhcp**

步骤 7 在 防火墙管理中心 中，禁用管理连接，在 **设备 (Devices) 设备管理 (Device Management)** 设备 (Device) 管理 (Management) 部分中更新 Firewall Threat Defense 的**远程主机地址 (Remote Host Address)**IP 地址 (IP address) 和可选**辅助地址 (Secondary Address)**，然后重新启用连接。**设备 > 设备管理**

请参阅更新防火墙管理中心中的主机名或 IP 地址，第 44 页。如果在将 Firewall Threat Defense 添加到 防火墙管理中心 时使用了 Firewall Threat Defense 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

步骤 8 确保管理连接已重新建立。

在 防火墙管理中心 中，检查 **设备 (Devices) 设备管理 (Device Management) 设备 (Device)** 管理 (Management)状态 (Status)字段上的管理连接状态或查看 **设备 > 设备管理** 中的通知。防火墙管理中心

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 64 页。

查看数据接口管理的管理器访问详细信息

当使用数据接口进行 防火墙管理中心 管理而不是使用专用管理接口时，必须注意在 防火墙管理中心 中更改设备的接口和网络设置，以免中断连接。您也可以在设备上本地更改数据接口设置，这就要求您在 防火墙管理中心 中手动协调这些更改。**设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 设备管理 (Management) > 管理器访问 + 配置详细信息 (Manager Access - Configuration Details)** 对话框可帮助您解决 防火墙管理中心 和 Firewall Threat Defense 本地配置之间的任何差异。

通常，在将 Firewall Threat Defense 添加到 防火墙管理中心 之前，您可以作为初始 Firewall Threat Defense 设置的一部分来配置管理器访问数据接口。当您将 Firewall Threat Defense 添加到 防火墙管理中心时， 防火墙管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。对于 DNS 服务器，如果在注册期间发现了它，则在本地维护配置，但不会将其添加到 防火墙管理中心 中的平台设置策略。

将 Firewall Threat Defense 添加到 防火墙管理中心 后，如果使用 **configure network management-data-interface** 命令在 Firewall Threat Defense 上本地更改数据接口设置，则 防火墙管理中心 会检测到配置更改，并阻止部署到 Firewall Threat Defense。防火墙管理中心 会使用以下方法之一来检测配置更改：

- 部署到 Firewall Threat Defense。在部署 防火墙管理中心 之前，它将检测配置差异并停止部署。
- **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框上的**刷新 (Refresh)** 按钮

要删除阻止，您必须转到**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)**. 下次部署时，防火墙管理中心 配置将覆盖 Firewall Threat Defense 上任何剩余的冲突设置。在您重新部署之前，您有责任在 防火墙管理中心 中手动修复配置。

请参阅此对话框中的以下页面。

配置

查看 防火墙管理中心 和 Firewall Threat Defense 上的管理器访问数据接口的配置对比。

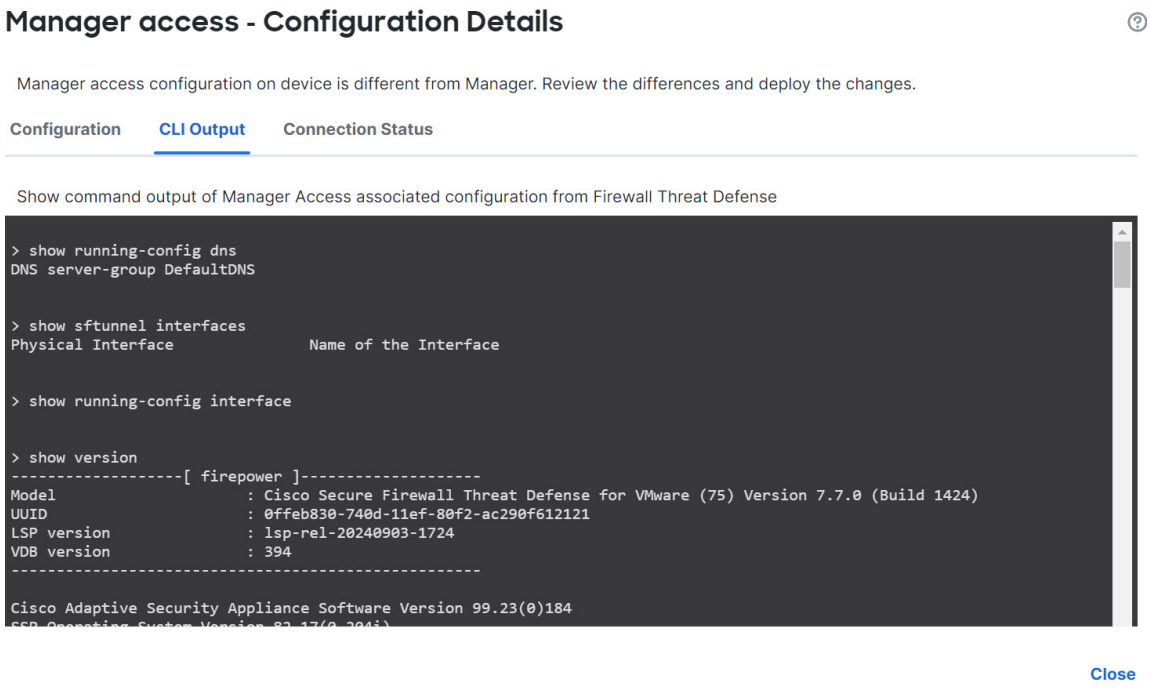
以下示例显示了在 Firewall Threat Defense 上输入 **configure network management-data-interface** 命令的位置的 Firewall Threat Defense 配置详细信息。以粉红色突出显示的内容显示了如果您**确认**差异但不匹配 防火墙管理中心 中的配置，则 Firewall Threat Defense 配置将被删除。以蓝色突出显示的内容显示了将在 Firewall Threat Defense 上修改的配置。以绿色突出显示的内容显示了将被添加到 Firewall Threat Defense 的配置。

以下示例显示在 防火墙管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。

CLI 输出

查看管理器访问数据接口的 CLI 配置，如果您熟悉底层 CLI，这将非常有用。

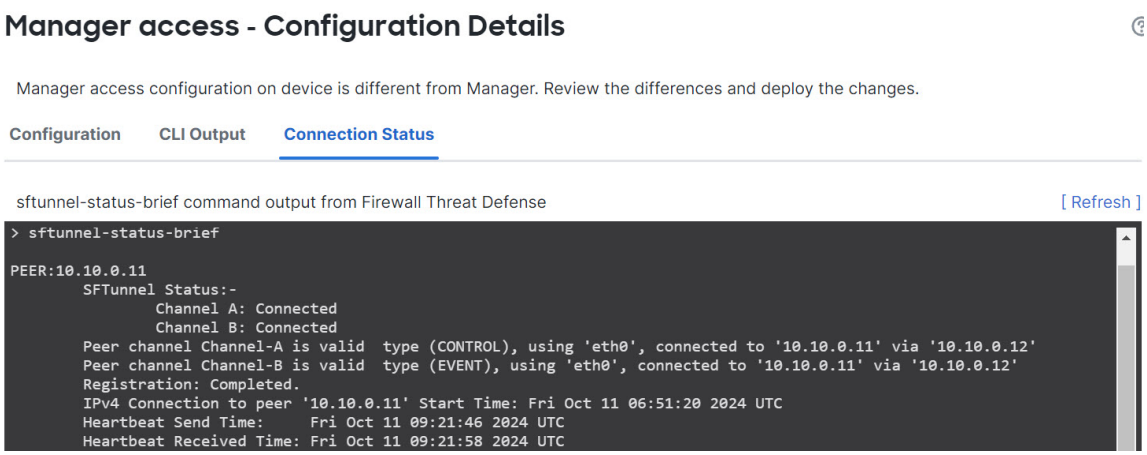
图 *48: CLI* 输出



连接状态

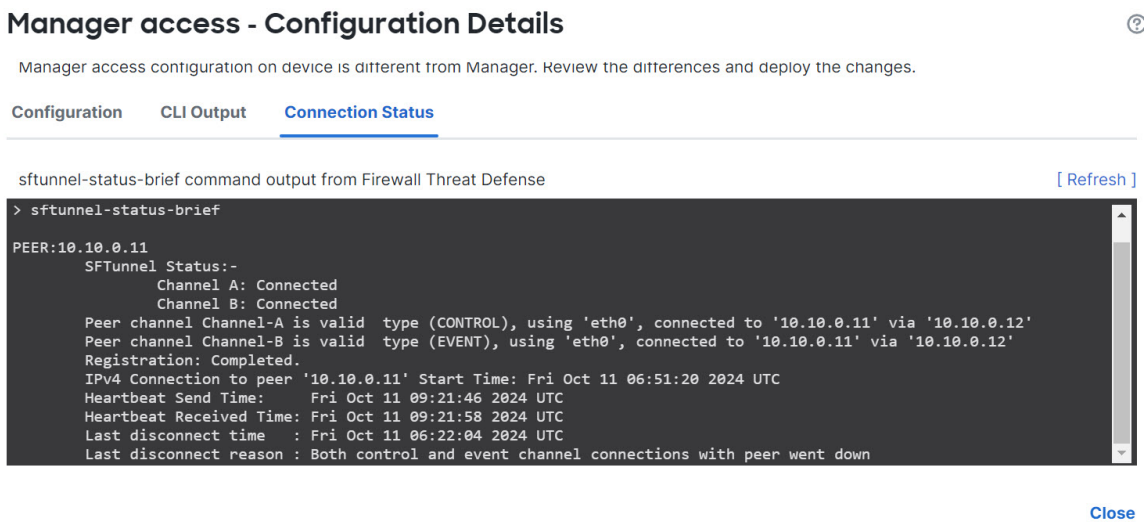
查看管理连接状态。以下示例显示了管理连接仍在使用管理“management0”接口。

图 *49:* 连接状态



以下状态显示数据接口成功连接，显示内部“ tap_nlp”接口。

图 *50:* 连接状态



请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
```

```
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

管理连接故障排除

-

如果防火墙管理中心断开连接，则手动回滚配置

如果将Firewall Threat Defense上的数据接口用于管理器访问，并从防火墙管理中心部署影响网络连接的配置更改，则可以将Firewall Threat Defense上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整防火墙管理中心中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

或者，如果在部署后失去连接，您可以启用配置的自动回滚；请参阅 编辑部署设置，第 75 页。

请参阅以下准则：

- 只有以前的部署可以在 Firewall Threat Defense 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 回滚只会影响您可以在防火墙管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 Firewall Threat Defense CLI 中进行配置。请注意，如果您在上次防火墙管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 防火墙管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 在 Firewall Threat Defense CLI 中，回滚到之前的配置。

configure policy rollback

回滚后，Firewall Threat Defense 会通知 防火墙管理中心 已成功完成回滚。在 防火墙管理中心 中，部署屏幕将显示一条横幅，说明配置已回滚。

注释

如果回滚失败且 防火墙管理中心 管理已恢复，请参阅https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html以了解常见的部署问题。在某些情况下，恢复 防火墙管理中心 管理访问权限后回滚可能会失败；在这种情况下，您可以解决 防火墙管理中心 配置问题，并从 防火墙管理中心 重新部署。

示例：

对于使用数据接口进行管理器访问的 Firewall Threat Defense ：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

步骤 2 检查管理连接是否已重新建立。

在 防火墙管理中心中，在连接状态 (Connection Status) 页面上检查管理连接状态。导航到 **设备** > **设备管理** ，然后导航到 **设备** 选项卡下的 **管理 (Management)** 区域。**在 设备 (Device)** 区域中，点击管理器访问详细信息：配置 (Manager Access Details: Configuration)FMC 访问：配置 (FMC Access: Configuration)，然后点击连接状态 (Connection Status)。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 64 页。

排除数据接口上的管理连接故障

当使用数据接口进行管理器访问而不是使用专用管理接口时，必须注意在 防火墙管理中心 中更改 Firewall Threat Defense 的接口和网络设置，以免中断连接。如果在将 Firewall Threat Defense 添加到 防火墙管理中心 后更改管理接口类型（从数据到管理，或从管理到数据），如果接口和网络设置未正确配置，则可能会丢失管理连接。

本主题可帮助您排除管理连接丢失的问题。

查看管理连接状态

在防火墙管理中心中，在**设备** > **设备管理**页面上检查管理连接状态。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

查看 Firewall Threat Defense 网络信息

在 Firewall Threat Defense CLI 上，查看管理和管理器访问数据接口网络设置：

show network

```
> show network
===============[ System Information ]===============
Hostname                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.4
Netmask                   : 255.255.255.192
Gateway                   : 169.254.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
```

```
DNS Servers               : 72.163.47.11
Interfaces                : Ethernet1/1

==================[ Ethernet1/1 ]==================
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:A4
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.6
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

检查向 防火墙管理中心注册 Firewall Threat Defense

在 Firewall Threat Defense CLI 中，检查 防火墙管理中心 注册是否已完成。请注意，此命令不会显示管理连接的 当前 状态。

show managers

```
> show managers
Type                      : Manager
Host                      : 16a3893c-caa7-11ee-8436-0925c06e7608DONTRESOLVE
Display name              : manager-1707852946.80444
Version                   : 7.6.0 (Build 1385)
Identifier                : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Registration              : Completed
Management type           : Configuration and analytics
```

Ping the 防火墙管理中心

在 Firewall Threat Defense CLI 上，使用以下命令从数据接口对 防火墙管理中心 执行 ping 操作：

ping *fmc_ip*

在 Firewall Threat Defense CLI 上，使用以下命令从管理接口对 防火墙管理中心 执行 ping 操作，该接口应通过背板路由到数据接口：

ping system *fmc_ip*

捕获 Firewall Threat Defense 内部接口上的数据包

在 Firewall Threat Defense CLI 上，捕获内部背板接口 (nlp_int_tap) 上的数据包，以查看是否发送了管理数据包：

capture 名称 **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

检查内部接口状态，统计信息和数据包计数

在 Firewall Threat Defense CLI 上，查看有关内部背板接口 nlp_int_tap 的信息：

show interface detail

```
> show interface detail
[...]
```

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

检查路由和 NAT

在 Firewall Threat Defense CLI 中，检查是否已添加默认路由 (S *)，以及管理接口 (nlp_int_tap) 是否存在内部 NAT 规则。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

检查其他设置

请参阅以下命令以检查是否存在所有其他设置。您还可以在防火墙管理中心的**设备** > **设备管理**页面上看到许多这些命令。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

检查 DDNS 更新是否成功

在 Firewall Threat Defense CLI 中，检查 DDNS 更新是否成功：

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

如果更新失败，请使用 **debug http** 和 **debug ssl** 命令。对于证书验证失败，请检查是否已在设备上安装根证书：

show crypto ca certificates *trustpoint_name*

要检查 DDNS 操作，请执行以下操作：

show ddns update interface *fmc_访问_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

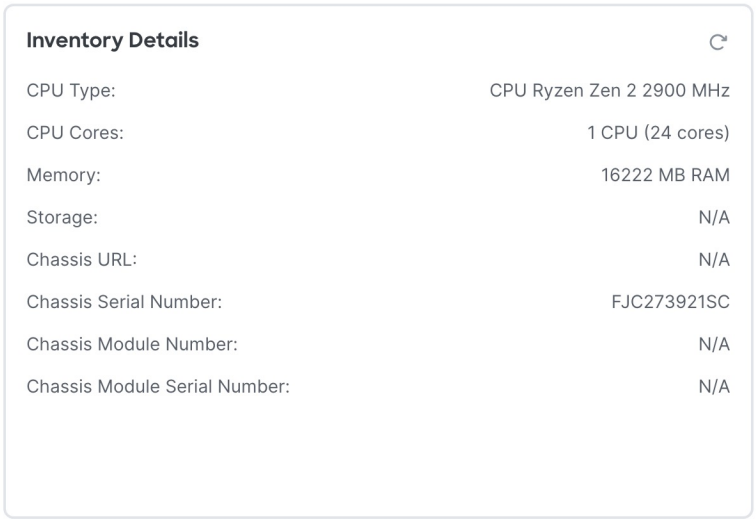
检查 防火墙管理中心 日志文件

请参阅 https://cisco.com/go/fmc-reg-error。

查看清单详细信息

设备 (Device) 页面上的**清单详细信息 (Inventory Details)** 部分会显示机箱详细信息，例如 CPU 和内存。

图 *51:* 设备清单详细信息



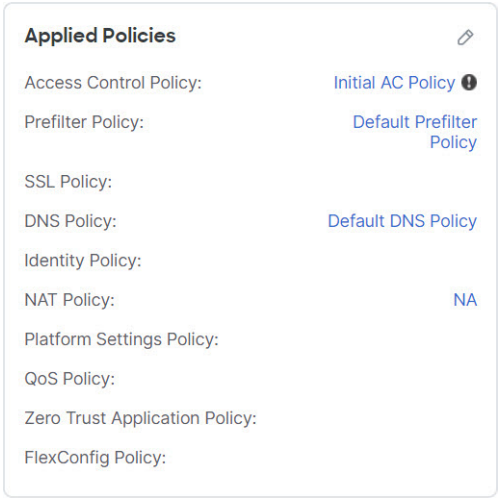
此部分显示机箱序列号。防火墙包含两个序列号：机箱序列号和 PCB（电路板）序列号。PCB 序列号显示在系统部分中。Firewall Threat Defense Virtual 没有机箱序列号。

要更新信息，请点击 **刷新** ()。

编辑应用的策略

设备 (Device) 页面的**应用的策略 (Applied Policies)** 部分显示了应用于防火墙的以下策略：

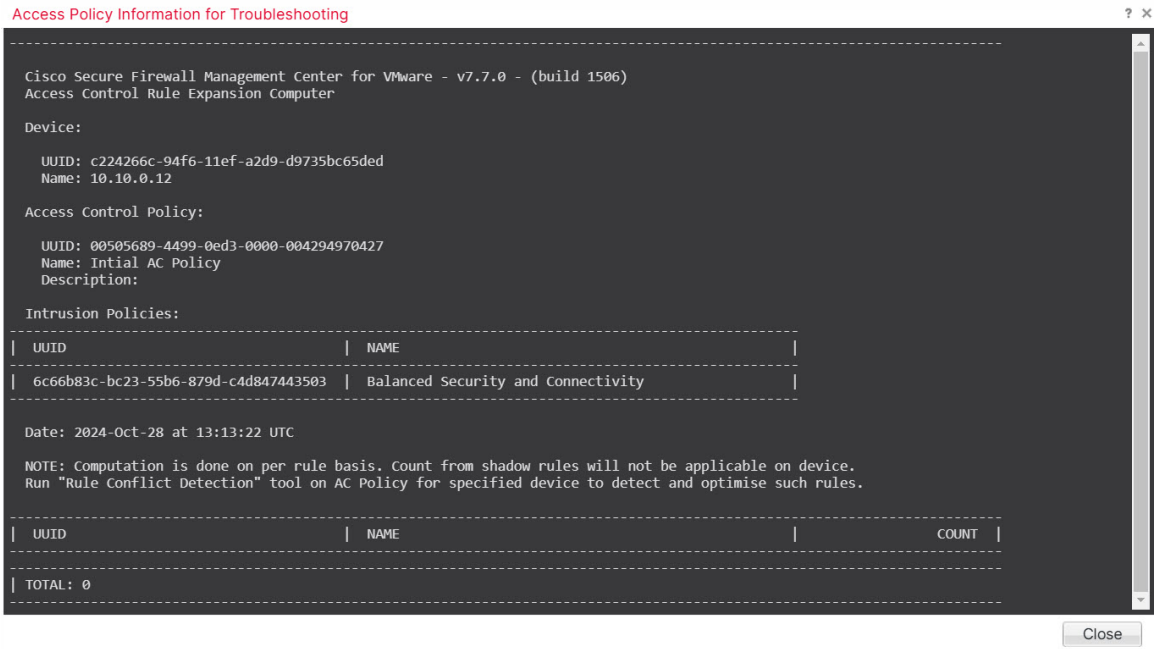
图 ***52:*** 应用的策略



对于包含链接的策略，您可以点击链接以查看策略。

对于访问控制策略，请点击 **感叹号 (!)** 图标以查看**用于故障排除的访问策略信息 (Access Policy Information for Troubleshooting)** 对话框。该对话框显示了如何将访问规则扩展为访问控制条目 (ACE)。

图 ***53:*** 用于故障排除的访问策略信息



您可以从**设备管理 (Device Management)** 页面将策略分配给单个设备。

过程

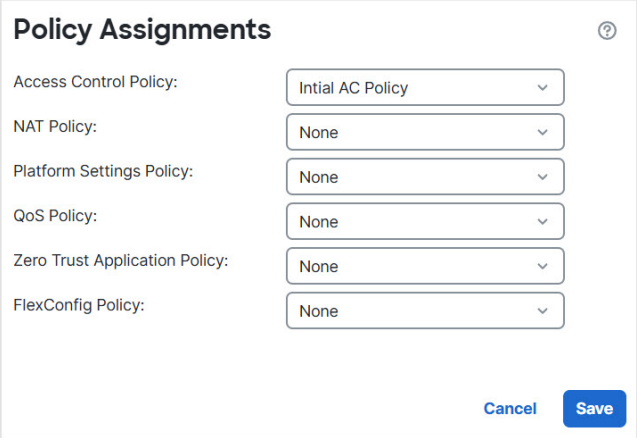
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑** ()。

步骤 3 点击**设备 (Device)**。

步骤 4 在 **应用的策略** 部分中，点击 **编辑** ()。

图 *54:* 策略分配



步骤 5 对于每种策略类型，请从下拉菜单选择一个策略。只有现有的策略会被列出。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

编辑高级设置

设备 (Device) 页面的**高级设置 (Advanced Settings)** 部分会显示高级配置设置表，如下所述。您可以编辑任何这些设置。

表 *5:*“高级”*(Advanced)* 部分表字段

字段	说明
应用绕行	设备上“自动应用绕行”的状态。

字段	说明
旁路阈值	“自动应用绕行”阈值（以毫秒为单位）。
对象组搜索	设备上对象组搜索的状态。运行时，FTD 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 Firepower 管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。 注释 默认情况下，当您首次在管理中心添加威胁防御时，将启用**对象组搜索 (Object Group Search)**。
接口对象优化	设备上的接口对象优化状态。部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

以下主题介绍如何编辑高级设备设置。

注释 有关“传输数据包”(Transfer Packets) 设置的信息，请参阅编辑常规设置，第 1 页。

配置自动应用旁路

自动应用绕行 (AAB) 允许数据包在 Snort 关闭或时绕过检测，或者对于经典设备，如果数据包处理时间过长，则 。AAB 会导致 Snort 在故障发生后的十分钟内重新启动，并生成可用于分析 Snort 故障原因的故障排除数据。

注意 部分激活 AAB 会重启 Snort 进程，这会暂时中断对几个数据包的检测。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

请参阅以下行为：

Firewall Threat Defense 行为：如果 Snort 关闭，则在指定的计时器持续时间后触发 AAB。如果 Snort 已启用，则即使数据包处理超过配置的计时器，也不会触发 AAB。

经典设备行为：AAB 限制通过接口处理数据包所允许的时间。通过网络的数据包延迟容限来平衡数据包处理时延。

该功能适用于任何部署；但在内联部署中最有价值。

通常，在超过延迟阈值后使用入侵策略中的“规则延迟阈值”通过快速路径传送数据包。“规则延迟阈值”不关闭引擎或生成故障排除数据。

如果绕过了检测，则设备会生成运行状况监控警报。

AAB 默认为禁用；要启用 AAB，请按照所述步骤进行操作。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要编辑高级设备设置的设备旁边，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)**，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑** (✎) 。

步骤 4 选中**自动应用旁路**。

步骤 5 输入介于 250 毫秒到 60,000 毫秒之间的**旁路阈值**。默认设置为 3000 毫秒 (ms)。

步骤 6 点击**保存**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

配置对象组搜索

运行时，Firewall Threat Defense 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 防火墙管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。

启用对象组搜索可以降低包含网络或接口对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

默认情况下会为在防火墙管理中心中首次添加的威胁防御设备启用对象组搜索。对于升级的设备，如果设备配置了禁用的对象组搜索，则需要手动将其启用。一次只能在一台设备上启用；您无法将其全局启用。我们建议您在部署使用网络或接口对象的访问规则的任何设备上将其启用。

注释 如果您启用对象组搜索，然后配置并操作设备一段时间，请注意，随后禁用该功能可能会导致不良结果。如果禁用对象组搜索，现有访问控制规则将按照设备的运行配置进行扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。如果设备运行正常，则在启用对象组搜索后不应将其禁用。

开始之前

- 型号支持—Firewall Threat Defense
- 我们建议您同时在每台设备上启用事务提交。在设备 CLI 中，输入 **asp rule-engine transactional-commit access-group** 命令。
- 更改此设置可能会在设备重新编译ACL时中断系统操作。我们建议您在维护窗口期间更改此设置。
- 可以使用 **object-group-search threshold** 命令启用阈值，以有助于防止性能下降。使用阈值运行时，对于每个连接，将根据网络对象匹配源和目标IP地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。配置规则以防止过多的匹配项。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要配置规则的 Firewall Threat Defense设备旁，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)** 选项卡，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑** (✎) 。

步骤 4 选中**对象组搜索 (Object Group Search)**。

步骤 5 要使对象组搜索除网络对象外还适用于接口对象，请选中**接口对象优化 (Interface Object Optimization)**。

如果不选择**接口对象优化 (Interface Object Optimization)**，则系统会为每个源/接口对部署单独的规则，而不是使用规则中使用的安全区域和接口组。这意味着接口组不可用于对象组搜索处理。

步骤 6 点击**保存**。

配置接口对象优化

部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而为每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

默认情况下，接口对象优化处于禁用状态。一次只能在一台设备上启用；您无法将其全局启用。

注释 如果禁用接口对象优化，则现有访问控制规则将在不使用接口对象的情况下进行部署，但这样可能会延长部署时间。此外，如果启用了对象组搜索，则其优势将不会应用于接口对象，并且您可能会在设备的运行配置中看到访问控制规则的扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。

开始之前

型号支持—Firewall Threat Defense

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要配置规则的 Firewall Threat Defense设备旁，点击 **编辑** ()。

步骤 3 点击**设备 (Device)** 选项卡，然后点击**高级设置 (Advanced Settings)** 部分的 **编辑** () 。

步骤 4 选中**接口对象优化 (Interface Object Optimization)**。

步骤 5 点击**保存**。

编辑部署设置

设备 (Device) 页面上的**运行状况 (Deployment Settings)** 部分显示下表所述信息。

图 *55:* 部署设置

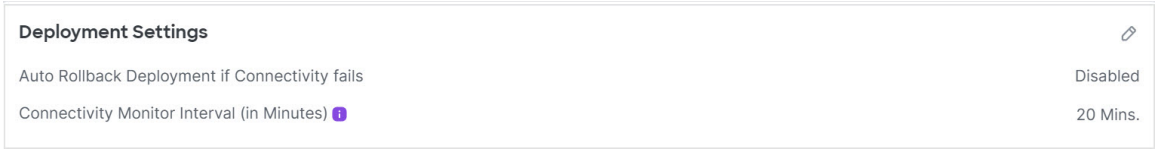


表 *6:* 部署设置

字段	说明
连接失败时自动回滚部署	“启用”(Enabled) 或“禁用”(Disabled)。 您可以在管理连接因部署而失败时启用自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。
连接监控间隔（分钟）	显示在回滚配置之前等待的时间。

您可以从**设备管理 (Device Management)** 页面设置部署设置。部署设置包括在管理连接因部署而失败时启用部署自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。您也可以使用 **configure policy rollback** 命令手动回滚配置（请参阅如果防火墙管理中心断开连接，则手动回滚配置，第 63 页）。

请参阅以下准则：

- 只有以前的部署可以在 Firewall Threat Defense 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。

- 回滚只会影响您可以在防火墙管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 Firewall Threat Defense CLI 中进行配置。请注意，如果您在上次防火墙管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 防火墙管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

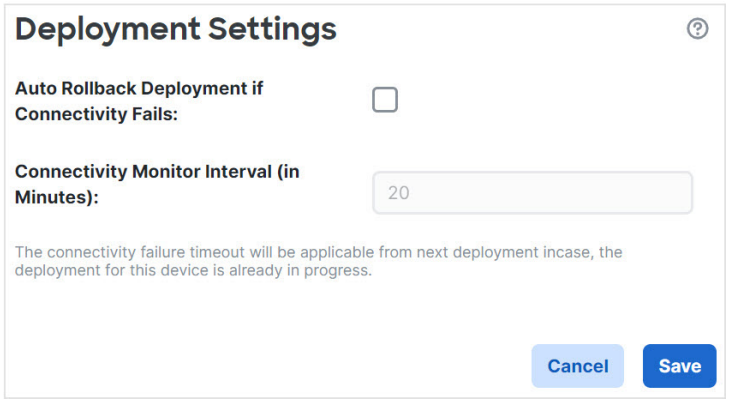
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)**。

步骤 4 在**部署设置 (Deployment Settings)** 部分中，点击 **编辑** (✎)。

图 *56:* 部署设置



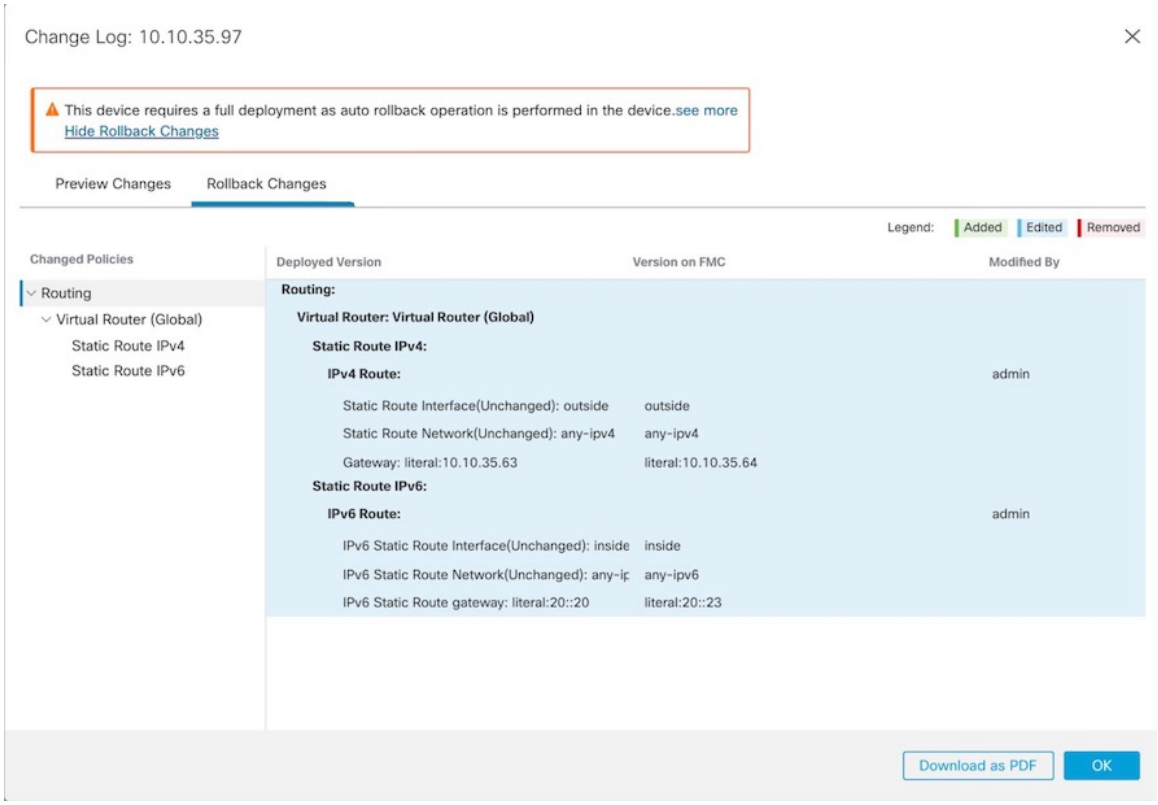
步骤 5 选中**连接失败时自动回滚部署 (Auto Rollback Deployment if Connectivity Fails)** 以启用自动回滚。

步骤 6 设置**连接监控间隔（分钟）(Connectivity Monitor Interval [in Minutes])** 以设置在回滚配置之前要等待的时间。默认值为 20 分钟。

步骤 7 如果发生回滚，请参阅以下内容以了解后续步骤。

- 如果自动回滚成功，您会看到一条成功消息，指示您执行完整部署。
- 您还可以转到 **部署 (Deployment)** **高级部署 (Advanced Deploy)** 屏幕，然后点击 **预览** (🔍) 图标以查看已回滚的配置部分（请参阅部署配置更改）。点击**显示回滚更改 (Show Rollback Changes)** 以查看更改，然后点击**隐藏回滚更改 (Hide Rollback Changes)** 以隐藏更改。

图 *57:* 回滚更改



- 在部署历史记录预览中，您可以查看回滚更改。请参阅查看部署历史记录。

步骤 8 检查管理连接是否已重新建立。

在防火墙管理中心中，检查连接状态页面上的管理连接状态。导航至**设备>设备管理**，然后在“**设备**”选项卡下的“**管理**”区域中，点击“**连接状态**”以查看“**连接状态**”页面。

在 Firewall Threat Defense CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅排除数据接口上的管理连接故障，第 64 页。

编辑集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *58:* 集群运行状况监控设置

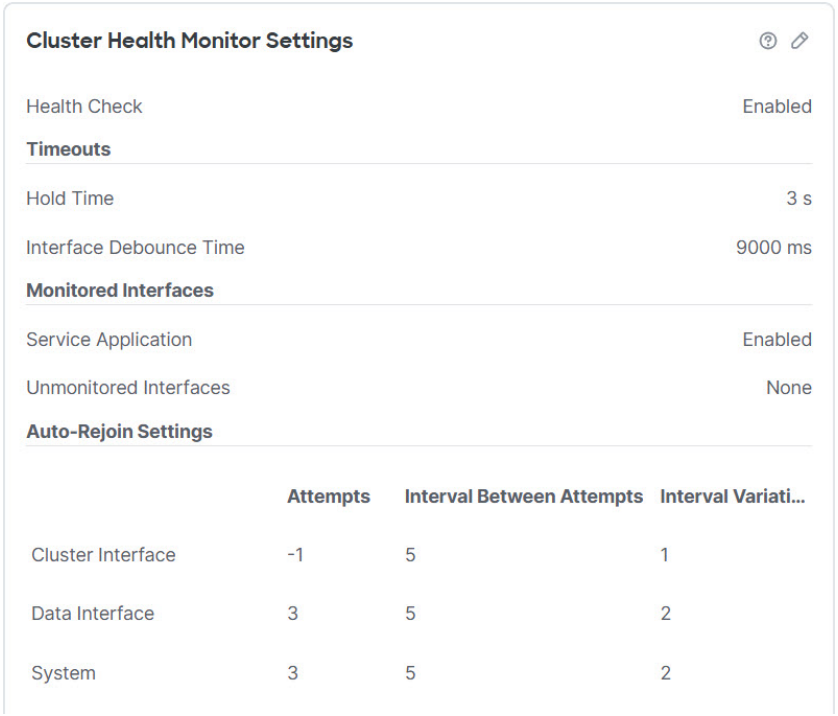


表 *7:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。

字段	说明
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。

注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

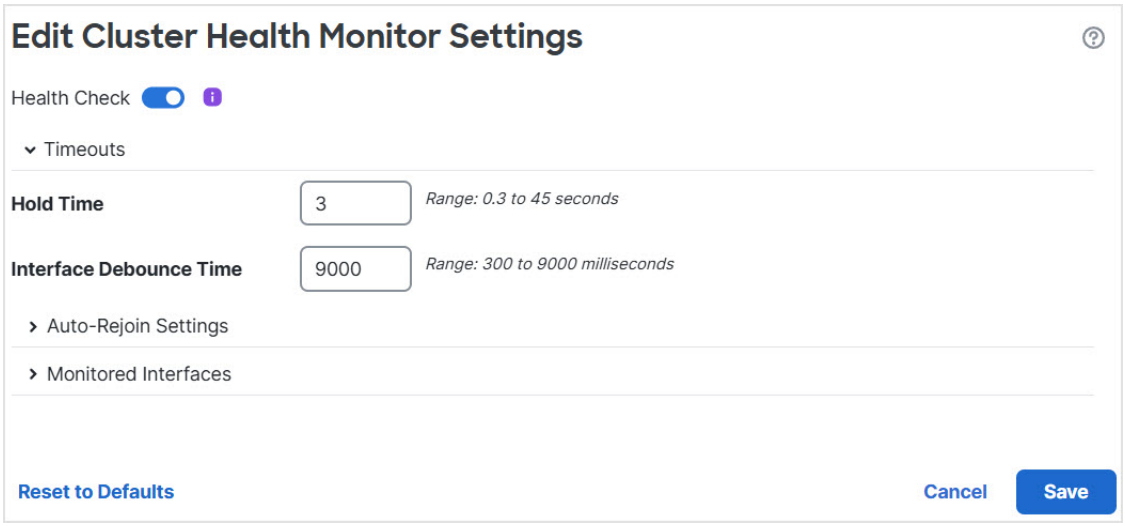
步骤 2 在要修改的集群旁边，点击 **编辑** (✎)。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** ()。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *59:* 禁用系统运行状况检查



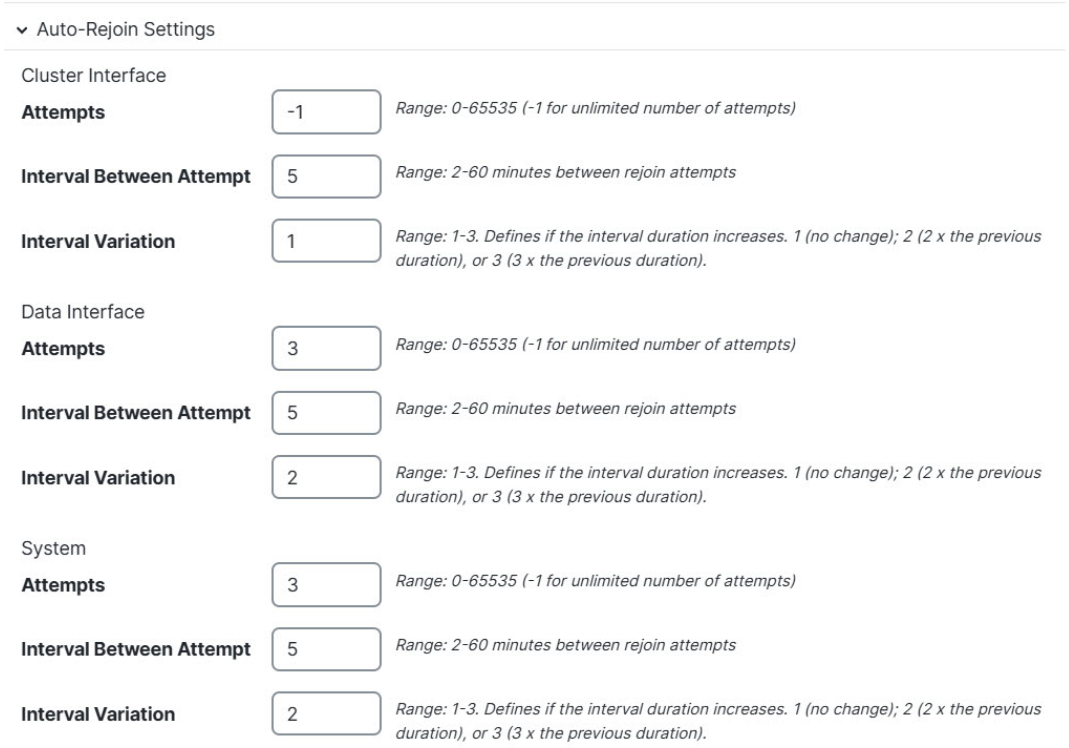
当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。
- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *60:* 配置自动重新加入设置

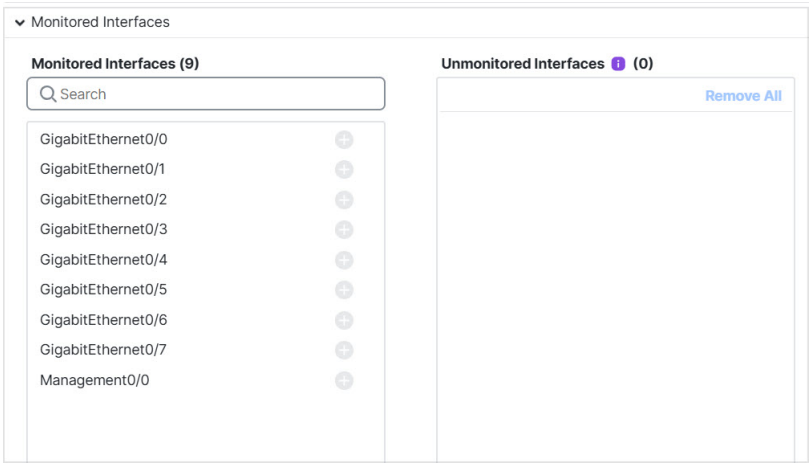


为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *61:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改。

热插拔 SSD

如果您有两个 SSD，它们会在您启动时形成 RAID。防火墙启动时，您可以在 CLI 上执行以下任务：Firewall Threat Defense

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

  当您在 Secure Firewall 设备中仅使用一块 SSD 时，**驱动器状态**将显示为**降级**。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

configure raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
> configure raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 operable
Presence:                    equipped
Lifecycle:                   available
Drive State:                 optimal
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    0
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                 nvme1n1
Disk State:                  in-sync
```

```
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

configure raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

configure raid add local-disk {**1** | **2**} *psid*

Psid 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。

禁用 USB 端口

默认情况下，type-A USB 端口已启用。出于安全考虑，您可能希望禁用 USB 端口访问。以下型号支持禁用 USB：

- Firepower 1000 系列
- Cisco Secure Firewall 200 系列
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100 系列

准则

- 启用或禁用 USB 端口需要 重新启动。
- 如果USB端口被禁用，并且您降级到不支持此功能的版本，则端口将保持禁用状态，并且在不清除 NVRAM 的情况下无法重新启用端口（FXOS local-mgmt **erase secure all** 命令）。
- 如果执行 ROMMON **factory-reset** 或 FXOS local-mgmt **erase secure**，USB 端口将重新启用。
- 对于高可用性 或集群，您必须在每台设备上单独禁用或重新启用端口。

注释 此功能不会影响 USB 控制台端口（如果有）。

禁用设备上的 USB 端口。

要禁用设备上的 USB 端口，您可以在 Firewall Threat Defense CLI 中执行此操作。

过程

步骤 1 禁用 USB 端口。

system support usb configure disable

reboot

要重新启用 USB 端口，请输入 **system support usb configure enable**。

示例：

```
>system support usb configure disable
USB Port Admin State set to 'disabled'.
Please reboot the system to apply any control state changes.

>reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

步骤 2 查看端口状态。

system support usb show

管理状态显示 USB 端口配置。运行状态显示当前操作。例如，如果禁用 USB 端口但不重新加载，则管理状态将显示为禁用，而运行状态将显示为启用。

示例：

```
>system support usb show
USB Port Info
---------------
Admin State: disabled
Oper State: disabled
```

在多实例模式下禁用 USB 端口

要在多实例模式下禁用 USB 端口，可以在 FXOS CLI 中执行此操作。

过程

步骤 1 禁用 USB 端口并重新启动，以使更改生效。

a) 禁用 USB 端口。

scope fabric-interconnect

disable usb-port

commit buffer

b) 重新启动机箱。

connect local-mgmt

reboot

示例：

```
firepower-4245 /fabric-interconnect # disable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

步骤 2 启用 USB 端口并重新启动，以使更改生效。

a) 启用 USB 端口。

scope fabric-interconnect

enable usb-port

commit buffer

b) 重新启动机箱。

connect local-mgmt

reboot

示例：

```
firepower-4245 /fabric-interconnect # enable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

步骤 3 查看 USB 端口状态。

scope fabric-interconnect

show usb-port

管理状态显示 USB 端口配置。运行状态显示当前操作。例如，如果禁用 USB 端口但不重新加载，则管理状态将显示为“已禁用”，而“运行状态”将显示为“启用”。

示例：

```
firepower-4245# scope fabric-interconnect
firepower-4245 /fabric-interconnect # show usb-port
Usb Port:
Equipment         Admin State Oper State
----------------- ----------- ----------
A                 Disabled    Disabled
```

为 FXOS 配置 SNMP

您可以为控制底层机箱功能的底层 FXOS 操作系统配置简单网络管理协议 (SNMP)。有关 Firewall Threat Defense 的 SNMP 配置，请参阅SNMP。

SNMP 是一种应用层协议，提供 SNMP 管理器和代理之间的通信消息格式。SNMP 提供用于监控和管理网络中的设备的标准化框架和通用语言。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来控制和监控网络设备的活动的系统。

- SNMP 代理 - 机箱内的软件组件，用于维护机箱的数据并根据需要向 SNMP 管理器报告数据。机箱包含代理和 MIB 集合。要启用 SNMP 代理并创建管理器和代理之间的关系，请在 防火墙管理中心 中启用并配置 SNMP。
- 管理信息库 (MIB) - SNMP 代理上的托管对象集合。

机箱支持 SNMPv1、SNMPv2c 和 SNMPv3。SNMPv1 和 SNMPv2c 使用基于社区的安全形式；SNMPv3 使用用户名和密码作为安全形式。

为 FXOS 启用 SNMP

启用 SNMP 并配置设置。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 点击 **SNMP**。

步骤 3 填写以下字段：

名称	说明
管理状态 (Admin State) 复选框	SNMP 已启用还是已禁用。仅当系统包含与 SNMP 服务器的集成时才启用此服务。
端口字段	Firepower 机箱与 SNMP 主机通信时使用的端口。无法更改默认端口。

名称	说明
社区字段	Firepower机箱在它发送给SNMP主机的任何陷阱消息中包含的默认 SNMPv1 或 v2 社区名或 SNMP v3 用户名和密码。 请为 SNMPv1 和 SNMPv2 输入有效的社区字符串： • 字母数字字符串和特殊字符集，长度在 1 - 32 个字符之间。（感叹号）、-（连字符）、~（代字号）、&&（双与号）、[ ]（方括号）、^（克拉）、'（单引号）、 "（双引号）和 < >（尖括号） ）。 • 请勿使用 @（at 号）、\（反斜线）、?（问号）或空格。 • 字符串也可以是 0x21 到 0x7E 范围内的 ASCII 字符，不包括 HTML 插词向量，即单引号 (')、双引号 (") 和尖括号 (< >)。 输入 SNMPv3 的有效用户名和密码： • 用户名可以是字母数字字符串，并且可以包含@（at符号）、\（反斜线）。（句点）、_（下划线）和 -（连字符）。 • 密码限制与社区字符串限制相同。 请注意，如果**社区**字段已设置，空字段右侧会显示文本**已设置：是**。如果**社区**字段尚未填充值，空字段右侧会显示文本**已设置：否**。
系统管理员名称字段	负责 SNMP 实施的联系人。 输入一个字符串，最多 255 个字符，例如邮件地址或姓名和电话号码。
位置字段	SNMP 代理（服务器）运行所在的主机的位置。 输入一个字母数字字符串，最多 510 个字符。

步骤 4 点击**保存**。

下一步做什么

创建 SNMP 陷阱和用户。

为 FXOS 创建 SNMP 陷阱

创建 SNMP 陷阱

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **SNMP**。

步骤 3 在 **SNMP 陷阱配置 (SNMP Traps Configuration)** 区域中，点击**添加 (Add)**。

步骤 4 在 **SNMP 陷阱配置**对话框中，填写以下字段：

名称	说明
主机名 (Host Name) 字段	Firepower 机箱应向其发送陷阱的 SNMP 主机的主机名或 IP 地址。
社区字段	向 SNMP 主机发送陷阱时，Firepower 机箱包含的 SNMP v1 或 v2 社区名或 SNMP v3 用户名。这必须与为 SNMP 服务配置的社区或用户名相同。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。
端口字段	Firepower 机箱与 SNMP 主机通信以布设陷阱时使用的端口。 输入一个介于 1 和 65535 之间的整数。
版本 字段	用于陷阱的 SNMP 版本和型号。这可以是以下其中一项： • **V1** • **V2** • **V3**
类型字段	如果为版本选择 **V2** 或 **V3**，则是要发送的陷阱类型。这可以是以下其中一项： • **陷阱** • **告知 (Informs)**
权限字段	如果为版本选择 **V3**，与陷阱相关联的权限。这可以是以下其中一项： • **身份验证 (Auth)** - 有身份验证，但没有加密 • **无身份验证 (Noauth)** - 没有身份验证和加密 • **权限 (Priv)** - 有身份验证和加密

步骤 5 点击**确定 (OK)** 以关闭 **SNMP 陷阱配置 (SNMP Trap Configuration)** 对话框。

步骤 6 点击**保存**。

为 FXOS 创建 SNMP 用户

创建 SNMP 用户。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **SNMP**。

步骤 3 在 **SNMP 用户配置 (SNMP Users Configuration)** 区域中，点击**添加 (Add)**。

步骤 4 在 **SNMP 用户配置**对话框中，填写以下字段：

名称	说明
用户名字段	分配给 SNMP 用户的用户名。 最多输入 32 个字母或数字。名称必须以字母开始，也可以指定 _（下划线）、.（句点）、@（邮箱符号）和 -（连字符）。
授权语法类型字段	授权类型：**SHA**。
使用 AES-128 复选框	如果选中此复选框，则此用户使用 AES-128 加密。 **注释** SNMPv3 不支持 DES。如果未选中 AES-128 框，则不会进行隐私加密，任何配置的隐私密码都不会生效。
身份验证密码字段	用户的密码。
确认字段	用于确认目的的再次输入的密码。
加密密码字段	用户的隐私密码。
确认字段	用于确认目的的再次输入的隐私密码。

步骤 5 点击**确定 (OK)** 以关闭 **SNMP 用户配置 (SNMP User Configuration)** 对话框。

步骤 6 点击**保存**。

配置 ISA 3000 的报警

您可以配置思科 ISA 3000 设备上的报警系统，以便在出现不正常情况时发出警告。

关于告警

您可以将 ISA 3000 配置为在多种条件下发出报警。如果有任何条件与配置的设置不匹配，系统会触发报警，报警的报告方式为 LED、系统日志消息、SNMP 陷阱以及连接到报警输出接口的外部设备。默认情况下，触发的报警仅会发出系统日志消息。

您可以将报警系统配置为监控以下对象：

- 电源。
- 主温度传感器和辅助温度传感器。
- 报警输入接口。

ISA 3000 具有内部传感器、2 个报警输入接口以及 1 个报警输出接口。您可以将外部传感器（如门禁传感器）连接到报警输入接口，将外部报警设备（如蜂鸣器或指示灯）连接到报警输出接口。

报警输出接口是一个中继装置。根据报警条件，中继处于连接或断开状态。当处于连接状态时，连接至该接口的任何设备都将被激活。当中继处于断开状态时，会导致连接的任何设备都处于非活动状态。只要触发了报警，中继就会保持连接状态。

有关连接外部传感器和告警继电器的信息，请参阅《Cisco ASA 系列通用操作 CLI 配置指南》中的“Cisco ISA 3000 警报”一章。请参阅《Cisco ISA 3000 工业安全设备硬件安装指南》。

报警输入接口

您可以将报警输入接口（或触点）连接到外部传感器，例如检测门是否打开的传感器。

每个报警输入接口都有一个对应的 LED。这些 LED 负责传达每个报警输入的报警状态。您可以为每个报警输入配置触发器和严重性。除了 LED，您还可以配置触点来触发输出中继（用于激活外部报警），以发送系统日志消息和 SNMP 陷阱。

下表介绍与报警输入的报警条件所对应的 LED 状态。表中还介绍了启用这些报警输入响应时输出中继、系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	次要报警 - 红色长亮 重大报警 - 红色闪烁	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

告警输出接口

您可以将外部报警（如蜂鸣器或灯光）连接到报警输出接口。

报警输出接口充当一个中继，并且还有一个对应的 LED，用于传达连接到输入接口的外部传感器以及内部传感器（例如双电源和温度传感器）的报警状态。请配置哪些报警应该激活输出中继（如果有）。

下表介绍与报警条件对应的LED和输出中继的状态。表中还介绍了启用这些报警响应时系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	红色常亮	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

系统日志报警

默认情况下，触发任何报警时，系统都会发送系统日志消息。如果您不希望收到这些消息，可以禁用系统日志消息传递。

要让系统日志报警正常工作，您还必须启用诊断日志记录。选择 **设备** > **平台设置**，添加或编辑分配给设备的FTD平台设置策略，并在**系统日志**页面上配置目标和设置。例如，您可以配置系统日志服务器、控制台日志记录或内部缓冲区日志记录。

如果未启用诊断日志记录的目标，报警系统不清楚向何处发送系统日志消息。

SNMP 报警

您可以选择配置报警，将SNMP陷阱发送到SNMP服务器。要让SNMP陷阱报警正常使用，您还必须配置 SNMP 设置。

选择 **设备** > **平台设置**，添加或编辑分配给该设备的威胁防御平台设置策略，并在 **SNMP** 页面上启用 SNMP 并配置设置。

报警默认值

下表指定了报警输入接口（触点）、冗余电源和温度的默认值。

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
报警触点 1	启用	关闭状态	次要	Disabled	Disabled	已启用
报警触点 2	启用	关闭状态	次要	Disabled	Disabled	已启用
冗余电源（在启用时）	启用	—	—	Disabled	Disabled	已启用

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
温度	为主温度报警启用（高阈值和低阈值的默认值分别为 92°C 和 -40°C） 为辅助报警禁用。	—	—	为主温度报警启用	为主温度报警启用	为主温度报警启用

报警先决条件

型号支持

ISA 3000 上的 Firewall Threat Defense。

配置 ISA 3000 的报警

请使用 FlexConfig 为 ISA 3000 配置报警。以下主题介绍如何配置不同类型的报警。

配置报警输入触点

如果您将报警输入触点（接口）连接到外部传感器，可以将触点配置为基于传感器的输入发出报警。事实上，如果触点关闭，即电流停止流经触点，系统会默认启用触点来发送系统日志消息。只有当默认设置不符合您的要求时，才需要配置触点。

报警触点的编号分别是 1 和 2，您需要了解如何连接物理引脚以配置正确的设置。单独配置每个触点。

过程

步骤 1 创建 FlexConfig 对象以配置警报输入联系人。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Configure_Alarm_Contacts。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。

- **对象正文 (Object body)** - 在对象正文中，键入配置警报联系人所需的命令。以下步骤介绍了这些命令。

c) 配置报警触点的说明。

alarm contact {**1** | **2**} **description** *string*

例如，要将触点 1 的说明设置为“Door Open”，请输入以下命令：

```
alarm contact 1 description Door Open
```

d) 配置报警触点的严重性。

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

您可以指定 **any** 更改所有触点的严重性，而不是配置一个触点。严重性控制与触点关联的 LED 指示灯的行为。

- **major**- LED 指示灯红色闪烁。
- **minor**- LED 指示灯红色长亮。这是默认值。
- **none**- LED 指示灯熄灭。

例如，要将触点 1 的严重级别设置为“Major”，请输入以下命令：

```
alarm contact 1 severity major
```

e) 配置报警触点的触发器。

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

您可以指定 **any** 更改所有触点的触发器，而不是配置一个触点。触发器决定发出报警信号的电气条件。

- **open**- 触点的正常状态为闭合，即电流流经触点。如果触点变成打开状态，即电流停止流动，会触发警报。
- **closed**- 触点的正常状态为打开，即电流不通过触点。如果触点变成闭合状态，即电流开始流经触点，会触发警报。这是默认值。

例如，将门禁传感器连接到报警输入触点1，该触点的正常状态为没有电流流经报警触点（即打开）。如果门被打开，触点会变成闭合状态，电流将流经报警触点。您应将报警触发器设为关闭，以便当电流开始流动时，警报响起。

```
alarm contact 1 trigger closed
```

f) 配置触发报警触点时采取的操作。

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。

例如，要启用报警输入触点 1 的所有操作，请输入以下命令：

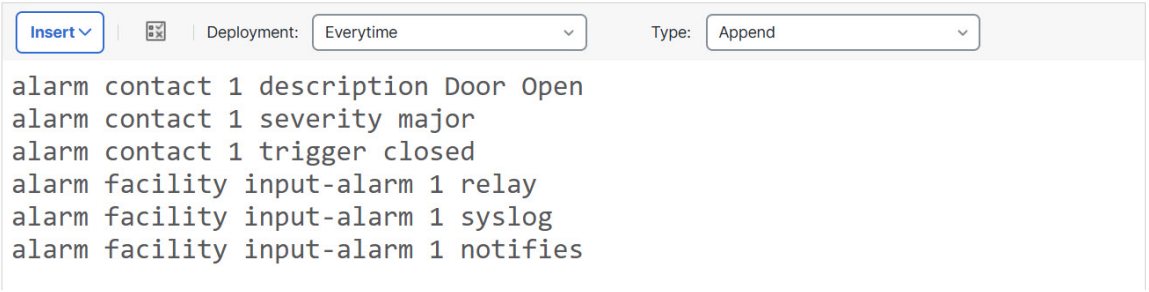
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

g) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

此对象正文应如下所示：



h) 点击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

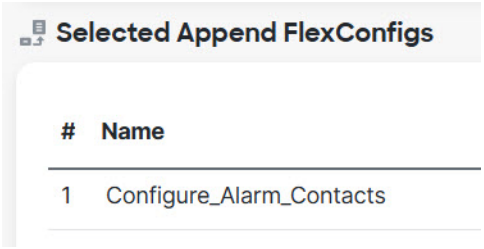
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择警报联系人 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于警报联系人命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置。

配置电源报警

ISA 3000 包含两个电源。默认情况下，系统在单电源模式下运行。但是，您可以配置系统在双电源模式下运行，其中第二个电源会在主电源发生故障时自动供电。启用双电源模式时，自动启用电源报警来发送系统日志警报，但您可以完全禁用警报，或同时启用 SNMP 陷阱或报警硬件中继。

以下过程说明如何启用双电源模式下，以及如何配置电源报警。

过程

步骤 1 创建 FlexConfig 对象以配置电源警报。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Power_Supply_Alarms。

- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置电源警报所需的命令。以下步骤介绍了这些命令。

c) 启用双电源模式。

power-supply dual

例如：

```
power-supply dual
```

d) 配置触发电源报警时要采取的操作。

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。
- **禁用** - 禁用电源报警。为电源报警配置的任何其他操作都无法运行。

例如，要启用电源报警的所有操作，请输入以下命令：

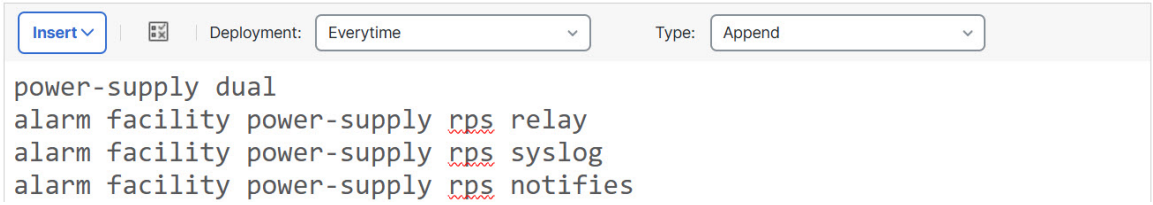
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

e) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

此对象正文应如下所示：



f) 点击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

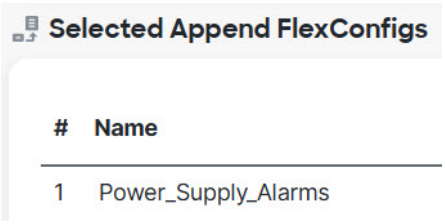
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择电源警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于电源警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置。

配置温度报警

您可以配置基于设备中 CPU 卡温度的警报。

您可以设置主要和辅助温度范围。如果温度低于低阈值，或超过高阈值，则触发报警。

默认对所有报警操作启用主温度报警：输出中继、系统日志和 SNMP。主要温度范围的默认设置为 -40°C 至 92°C。

默认情况下，禁用辅助温度报警。您可以将辅助温度范围设置为 -35°C 至 85°C。

由于辅助温度范围比主范围更严格，如果您设置辅助低温度或高温度，该设置将禁用对应的主要设置，即使您为主设置配置非默认值。您不能启用两个单独的高温度报警和两个单独的低温度报警。

因此，在实践中，您应为高温度和低温度仅配置主要设置或仅配置辅助设置。

过程

步骤 1 创建 FlexConfig 对象以配置温度警报。

a) 选择**对象** > **FlexConfig** > **FlexConfig 对象** 。

b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Configure_Temperature_Alarms。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入配置温度警报所需的命令。以下步骤介绍了这些命令。

c) 配置可接受的温度范围。

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

温度单位为摄氏度。主要报警的允许范围为 -40 至 92，这也是默认的范围。辅助报警的允许范围是 -35 到 85。低值必须小于高值。

例如，要设置更严格的 -20 至 80 温度范围（在辅助报警的允许范围内），请按如下所示配置辅助报警：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

d) 配置触发温度报警时要采取的操作。

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。
- **通知** - 发送 SNMP 陷阱。

例如，要启用辅助温度报警的所有操作，请输入以下命令：

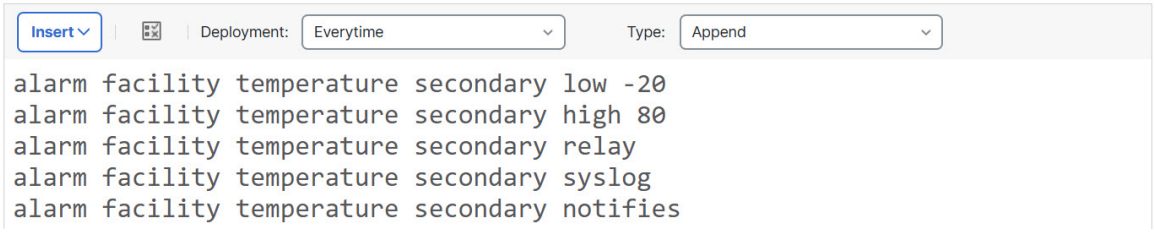
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

e) 验证对象正文是否包含您想要的命令。

例如，如果您的模板包含此过程中所示的所有命令示例，则对象正文将包含以下命令：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

此对象正文应如下所示：



f) 点击**保存**。

步骤 2 创建 FlexConfig 策略并将其分配给设备。

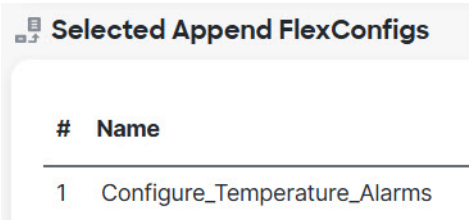
a) 选择**设备** > **+ 显示更多** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择温度警报 FlexConfig 对象，然后点击 **>** 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。
e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。
f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于温度警报命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置。

关闭外部告警

如果您使用连接到报警输出的外部报警，并触发了报警，可以使用 **clear facility-alarm output** 命令从设备 CLI 关闭外部报警。此命令会断开输出引脚，同时关闭输出 LED。

监控告警

以下主题介绍如何监控和管理报警。

监控报警状态

您可以在 CLI 中使用以下命令监控报警。

- **show alarm settings**

  显示每个可能的报警的当前配置。

- **show environment alarm-contact**

  显示输入报警触点的物理状态信息。

- **show facility-alarm relay**

  显示有关已触发输出中继的报警信息。

- **show facility-alarm status** [**info** | **major** | **minor**]

显示所有已触发报警的信息。您可以通过过滤 **major** 或 **minor** 状态来限制视图。**info** 关键字提供与不使用关键字时相同的视图。

监控报警系统日志消息

根据您配置的报警类型，您可能会看到以下系统日志消息。

双电源报警

- %FTD-1-735005：电源设备冗余正常
- %FTD-1-735006：电源设备冗余丢失

温度报警

在这些报警中，*Celsius* 将替换为设备上检测到的温度，以摄氏为单位。

- %FTD-6-806001：主要报警 CPU 温度高 *Celsius*
- %FTD-6-806002：CPU 高温主要报警已清除
- %FTD-6-806003：主要报警 CPU 温度低 *Celsius*
- %FTD-6-806004：CPU 低温主要报警已清除
- %FTD-6-806005：辅助报警 CPU 温度高 *Celsius*
- %FTD-6-806006：CPU 高温辅助报警已清除
- %FTD-6-806007：辅助报警 CPU 温度低 *Celsius*
- %FTD-6-806008：CPU 低温辅助报警已清除

报警输入触点报警

在这些报警中，*description* 是您所配置触点的说明。

- %FTD-6-806009：与 ALARM_IN_1 *alarm_1_description* 对应的报警已确定
- %FTD-6-806010：与 ALARM_IN_1 *alarm_1_description* 对应的报警已清除
- %FTD-6-806011：与 ALARM_IN_2 *alarm_2_description* 对应的警报已确定
- %FTD-6-806012：与 ALARM_IN_2 *alarm_2_description* 对应的报警已清除

设备设置历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息

恢复配置模式现在支持NAT命令以及其他接口命令	10.0.0	10.0.0	恢复配置模式现在支持：
			• **nat** 以及相关的 **object** 和 **object-group** 命令。
			• 请参阅以下命令：**interface**
			  • **duplex**
			  • **fec**
			  • **negotiate-auto**
			  • **speed**
			这些 **interface** 命令以及 **shutdown**不支持在集群控制链路或故障转移链路的恢复配置模式下使用。
			新增/修改的诊断 CLI (**system support diagnostic-cli**) 命令： **configure recovery-config**

查看可现场更换内存模块的清单详细信息	10.0.0	10.0.0	此版本为受支持的设备引入了可现场更换的内存模块资产。现在可以在“设备管理”界面的**系统**部分查看可现场更换内存模块的详细信息。清单详细信息包括运行状态，以提高内存模块的现场可维护性。 新增/修改的命令：**show inventory** 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**编辑 (✎)

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
恢复配置模式用于在防火墙管理中心上进行紧急设备上配置和带外配置检测	7.7.0	7.7.0	如果断开了与设备的管理连接，您可以直接通过设备 CLI 选择配置更改： • 如果使用数据接口进行管理器访问，则恢复管理连接 • 选择无法等到连接恢复后再进行的策略更改 在恢复管理连接后，防火墙管理中心将检测设备上的配置更改。它不会自动更新 防火墙管理中心 中的设备配置；您必须查看配置差异，确认设备配置不同，然后在部署之前在 防火墙管理中心 中手动进行相同的更改。 新增/修改的诊断 CLI (**system support diagnostic-cli**) 命令： **configure recovery-config** 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** **运行状况 (Health)** > **带外状态 (Out of Band Status)** **编辑** (✎)
通过冗余管理器访问数据接口支持高可用性	7.7.0	7.7.0	现在，您可以使用具有高可用性的冗余管理器访问数据接口。
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群运行状况监控设置。	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** 注释 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
冗余管理器访问数据接口。	7.3.0	7.3.0	在使用数据接口进行管理器访问时，您可以配置辅助数据接口，以便在主接口发生故障时接管管理功能。设备会使用SLA监控来跟踪包含两个接口的静态路由和ECMP区域的可行性，以便管理流量可以使用这两个接口。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **管理器访问 (Manager Access)**
策略支持回滚以实现高可用性设备。	7.2.0	7.2.0	**configure policy rollback** 命令支持高可用性设备。
导致管理连接丢失的部署的自动回滚。	7.2.0	7.2.0	如果部署导致管理中心和威胁防御之间的管理连接断开，您现在就可以启用配置的自动回滚。以前，您只能使用 **configure policy rollback** 命令手动回滚配置。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **部署设置 (Deployment Settings)** • **部署 (Deploy)** > **高级部署 (Advanced Deploy)** > **预览 (Preview)** • **部署 (Deploy)** > **部署历史 (Deployment History)** > **预览 (Preview)**
默认情况下会为访问控制规则启用对象组搜索。	7.2.0	7.2.0	从版本 7.2.0 开始，托管设备默认启用**对象组搜索 (Object Group Search)** 设置。在“设备管理”页面上编辑设备设置时，此选项位于 **高级设置 (Advanced Settings)** 部分中。

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
导入和导出设备配置。	7.1.0	7.1.0	您可以导出设备特定的配置，然后可以在以下使用案例中为同一设备导入已保存的配置： • 将设备移至其他 FMC。 • 恢复老旧配置。 • 重新注册设备。 新增/修改的屏幕： **设备** > **设备管理** > **设备** > **常规**
更新 FTD 上的 FMC IP 地址。	6.7.0	6.7.0	如果更改 FMC IP 地址，现在可以使用 FTD CLI 更新设备。 新增/经修改的命令： **configure manager edit**
思科 ISA 3000 系列的报警。	6.7	任意	已使用 FlexConfig 验证思科 ISA 3000 系列的警报配置。您应该能够在支持 FlexConfig 的旧版本中配置警报，但双电源警报除外。 支持的平台：ISA 3000 上的 Cisco Secure Firewall Threat Defense

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。

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。

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。