



设备管理

本指南适用于作为主要管理器或仅作为分析管理器的本地设备 Cisco Secure Firewall Management Center。在将思科防御协调器 (CDO) 云交付的防火墙管理中心用作主管理器时，您只能使用本地部署管理中心进行分析。请勿将本指南用于云交付的防火墙管理中心管理；请参阅[使用 思科防御协调器 中的云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense](#)。

您可以在 Cisco Secure Firewall Management Center 中添加和管理设备。

- [关于设备管理，第 1 页](#)
- [设备管理的要求和前提条件，第 10 页](#)
- [登录到设备的命令行界面，第 10 页](#)
- [为手动注册完成威胁防御初始配置，第 12 页](#)
- [管理设备，第 27 页](#)
- [交换机管理器，第 62 页](#)
- [Cisco Secure Firewall 3100/4200 上的热插拔 SSD，第 67 页](#)
- [禁用 USB 端口，第 70 页](#)
- [设备管理的历史记录，第 73 页](#)

关于设备管理

使用管理中心来管理您的设备。

关于管理中心和设备管理

在管理中心管理设备时，它会在自己和设备之间设置双向、SSL 加密的通信信道。管理中心使用此信道向设备发送有关如何分析和流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到管理中心。

通过使用管理中心管理设备，您可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地进行更改
- 在设备上安装各种类型的软件更新
- 向托管设备推送运行状况策略并从管理中心监控其运行状态



注释 如果您有CDO托管设备，并且仅将本地部署管理中心用于分析，则本地部署管理中心不支持策略配置或升级。本指南中与设备配置和其他不支持的功能有关的章节和程序不适用于主管理器为CDO的设备。

管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用管理中心来管理设备行为的几乎每个方面。



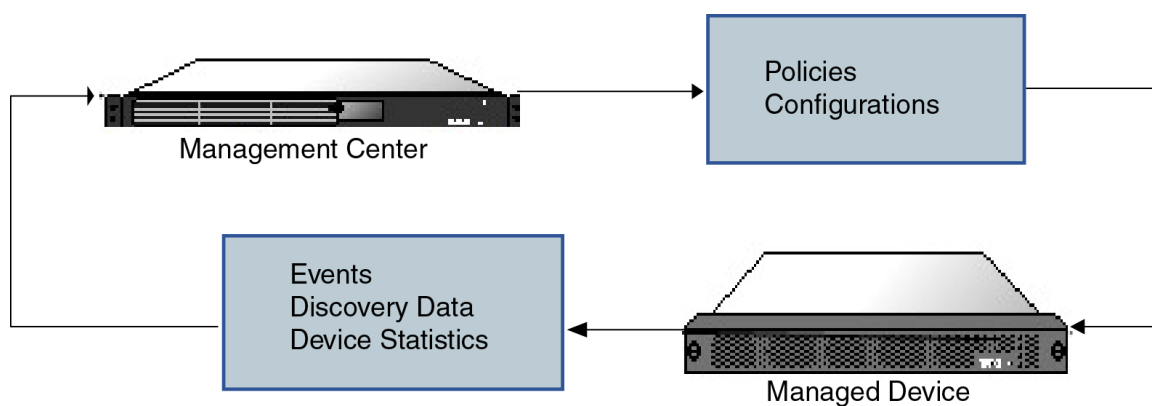
注释 尽管管理中心可以按照 <http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html> 中提供的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本威胁防御软件的新功能不适用于这些以前发布的设备。某些管理中心功能可能适用于早期版本。

Cisco Secure Firewall Management Center可以管理哪些内容？

您可以将 Cisco Secure Firewall Management Center 用作集中管理点来管理威胁防御设备。

管理设备时，信息通过 TLS-1.3-加密的安全隧道在管理中心和该设备之间传输。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

下图列出了在管理中心及其托管设备之间传输的内容。请注意，设备间发送的事件和策略的类型基于设备类型。



关于管理连接

使用管理中心信息配置设备并将设备添加到管理中心后，设备或管理中心可以建立管理连接。根据初始设置：

- 设备或管理中心都可以启动。

- 只有设备可以启动。
- 只有管理中心可以发起。

启动始终使用管理中心上的 `eth0` 或设备上编号最低的管理接口。如果未建立连接，则会尝试其他管理接口。管理中心上的多个管理接口可让您连接到离散网络或隔离管理和事件流量。但是，发起方不会根据路由表选择最佳接口。

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。默认情况下，管理连接使用 TCP 端口 8305（此端口可配置）。如果您在设备和管理中心之间放置另一个威胁防御，为了防止潜在的管理中断，请务必通过为其应用预过滤器策略来豁免管理流量执行深度检查。



注释 管理连接是信道自身与设备之间的 TLS-1.3 加密的安全通信信道。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

除策略和事件以外的其他功能

除将策略部署到设备和从其接收事件以外，还可以在管理中心上执行其他设备相关任务。

备份设备

您无法从 FTD CLI 备份物理托管设备。要备份配置数据和（可选的）统一文件，请使用管理设备的管理中心来执行设备备份。

要备份事件数据，请对管理设备的管理中心执行备份。

更新设备

思科会不定期发布 Firepower 系统更新，包括：

- 入侵规则更新，其中可能包含新的和已更新的入侵规则
- 漏洞数据库 (VDB) 更新
- 地理位置更新
- 软件补丁和更新

可以使用管理中心在其管理的设备上安装更新。

关于设备管理接口

每个设备都包含一个用于与管理中心通信的管理接口。您可以选择将设备配置为使用数据接口进行管理，而不是专用的管理接口。

您可以在管理接口或控制台端口上执行初始设置。

管理接口还用于与智能许可服务器通信、下载更新以及执行其他管理功能。

威胁防御上的管理和事件接口

设置设备时，指定要连接到的管理中心 IP 地址或主机名称（如已知）。如果设备启动了连接，管理和事件流量都在初始注册时转到此地址。如果管理中心未知，则管理中心建立初始连接。在这种情况下，它最初可能从与威胁防御上指定的不同的管理中心管理接口连接。后续连接应使用具有指定 IP 地址的管理中心管理接口。

如果管理中心具有单独的仅事件接口，则托管设备会在网络允许的情况下将后续事件流量发送到管理中心仅事件接口。此外，某些托管设备型号包括一个额外的管理接口，您可以为仅事件流量配置该接口。请注意，如果您配置用于管理的数据接口，则不能使用单独的管理接口和事件接口。如果事件网络关闭，则事件流量将恢复到管理中心和/或托管设备上的常规管理接口。

使用威胁防御数据接口进行管理

您可以使用专用的管理接口或常规数据接口与管理中心通信。如果想要从外部接口远程管理威胁防御，或者您没有单独的管理网络，则在数据接口上进行管理器访问非常有用。此外，使用数据接口可以配置冗余辅助接口，以便在主接口发生故障时接管管理功能。

管理器访问要求

从数据接口进行管理器访问遵循以下要求。

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 **EtherChannel**，也不能在管理器访问接口上创建子接口。您还可以使用 管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 威胁防御 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用管理中心来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 threat defense virtual，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。

高可用性要求

将数据接口与设备高可用性配合使用时，请参阅以下要求。

- 在两台设备上使用相同的数据接口进行管理器访问。
- 不支持冗余管理器访问数据接口。
- 不能使用 DHCP；仅支持静态 IP 地址。无法使用依赖 DHCP 的功能，包括 DDNS 和零接触调配。
- 在同一子网中有不同的静态 IP 地址。
- 使用 IPv4 或 IPv6；不能同时设置。
- 使用相同的管理器配置（**configure manager add** 命令）确保连接相同。
- 不能将数据接口用作故障切换链路或状态链路。

每个设备型号的管理接口支持

有关管理接口位置，请参阅您的型号的硬件安装指南。



注释 对于 Firepower 4100/9300，MGMT 接口用于机箱管理，而不是用于 威胁防御逻辑设备管理。必须将单独的接口配置为 mgmt（和/或 firepower-eventing）类型，然后将其分配给 威胁防御 逻辑设备。

有关每个托管设备型号上支持的管理接口，请参阅下表。

表 1: 托管设备上的管理接口支持

型号	管理界面	可选的事件接口
Firepower 1000	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall 1200	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall 3100	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持

型号	管理界面	可选的事件接口
Cisco Secure Firewall 4200	management0 注释 management0 是管理 1/1 接口的内部名称。	management1 注释 management1 是管理 1/2 接口的内部名称。
Firepower 4100 和 9300	management0 注释 management0 是此接口的内部名称，与物理接口 ID 无关。	management1 注释 management1 是此接口的内部名称，与物理接口 ID 无关。
ISA 3000	br1 注释 br1 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall Threat Defense Virtual	eth0	不支持

设备管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置托管设备时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。



注释 用于管理接口的路由完全独立于您为数据接口配置的路由。如果配置用于管理的数据接口而不是使用专用管理接口，则流量将通过背板路由以使用数据路由表。本节中的信息不适用。

在某些平台上，可以配置多个管理接口（一个管理接口和一个仅事件接口）。默认路由不包括出口接口，因此选择的接口取决于您指定的网关地址以及网关属于哪个接口的网络。如果默认网络上有多个接口，设备将使用编号较低的接口作为出口接口。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到威胁防御的路由问题。



注释 用于管理连接的接口不由路由表决定。始终首先使用编号最低的接口来进行连接。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及重新分配源或目标 IP 地址。NAT 最常见的用途是允许专用网络与互联网进行通信。静态 NAT 执行 1:1 转换，这不会引发管理中心与设备的通信问题，但端口地址转换 (PAT) 更为常用。PAT 允许您使用单一的公共 IP 地址

和独特端口来访问公共网络；这些端口是根据需要动态分配的，因此您无法启动与 PAT 路由器后的设备的连接。

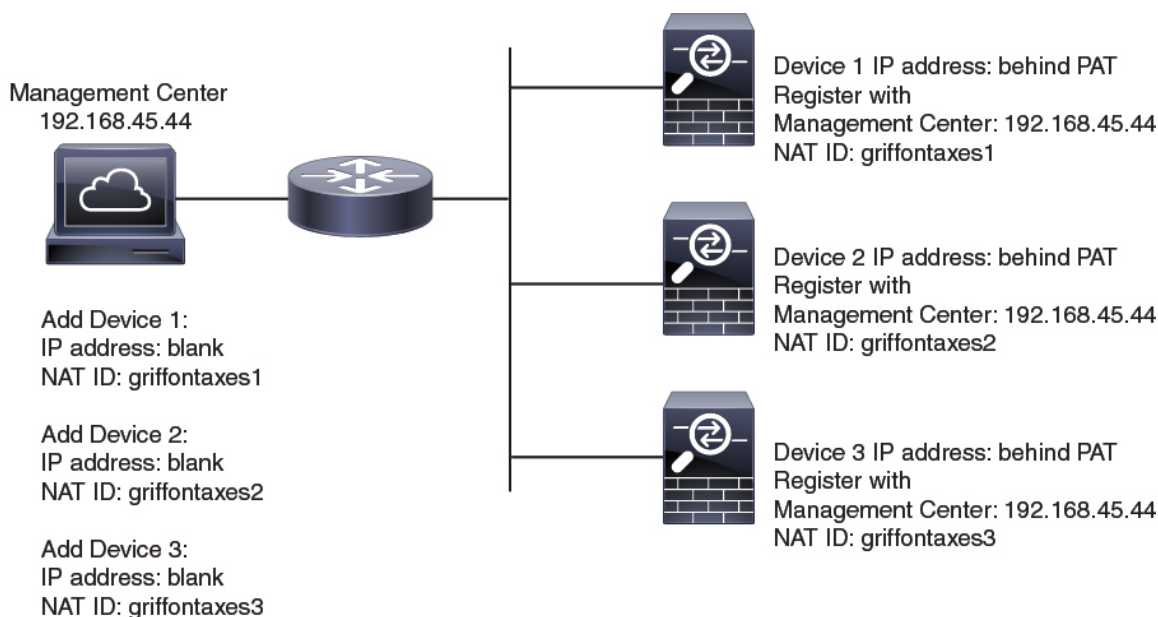
通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同同一个注册密钥）：管理中心当添加一个设备时，指定设备 IP 地址，设备指定管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

例如，您将设备添加到管理中心，但不知道设备 IP 地址（例如，设备在 PAT 路由器后），因此只需要在管理中心上指定 NAT ID 和注册密钥；将 IP 地址留空。在设备上，指定管理中心 IP 地址、相同的 NAT ID 和相同的注册密钥。设备将注册到管理中心的 IP 地址。此时，管理中心将使用 NAT ID 而不是 IP 地址对设备进行身份验证。

尽管 NAT ID 最常用于 NAT 环境，但您可以选择使用 NAT ID 来简化向管理中心添加多个设备的过程。在管理中心上，在将 IP 地址留空的同时为要添加的每个设备指定唯一的 NAT ID，然后在每个设备上指定管理中心 IP 地址和 NAT ID。注意：每个设备的 NAT ID 必须是唯一的。

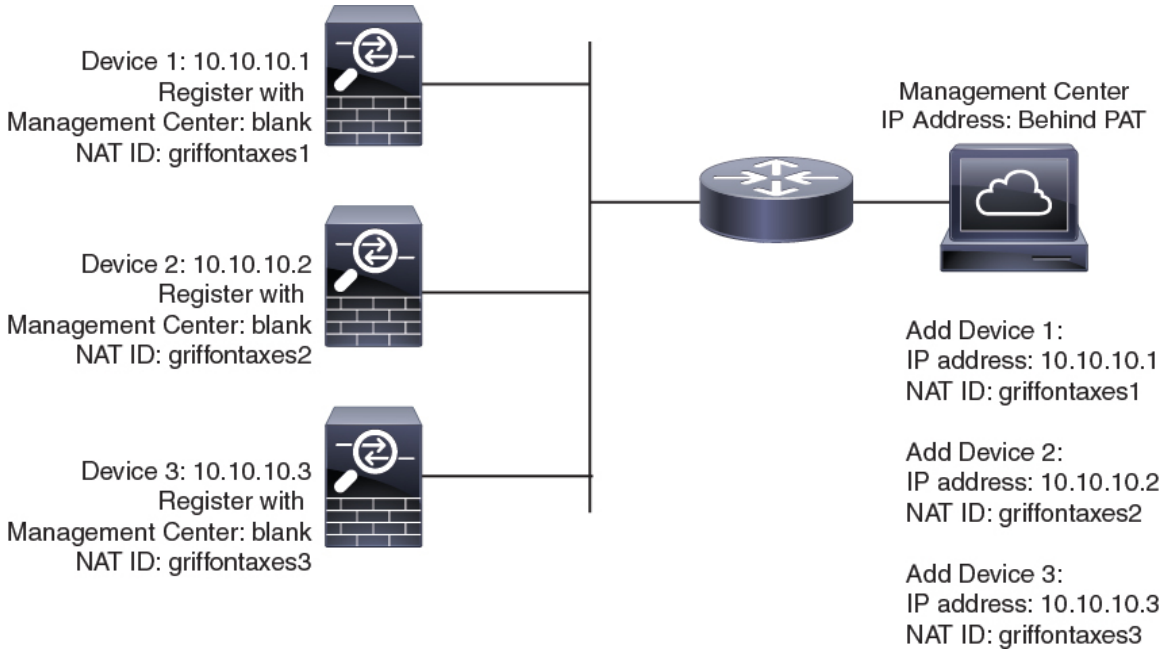
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在管理中心和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定管理中心 IP 地址。

图 1: PAT 后的托管设备 NAT ID



以下示例为 PAT IP 地址后的 管理中心。在这种情况下，在管理中心和这些设备上为每个设备指定一个唯一的 NAT ID，并在管理中心上指定设备 IP 地址。

图 2: PAT 后的 FMC NAT ID



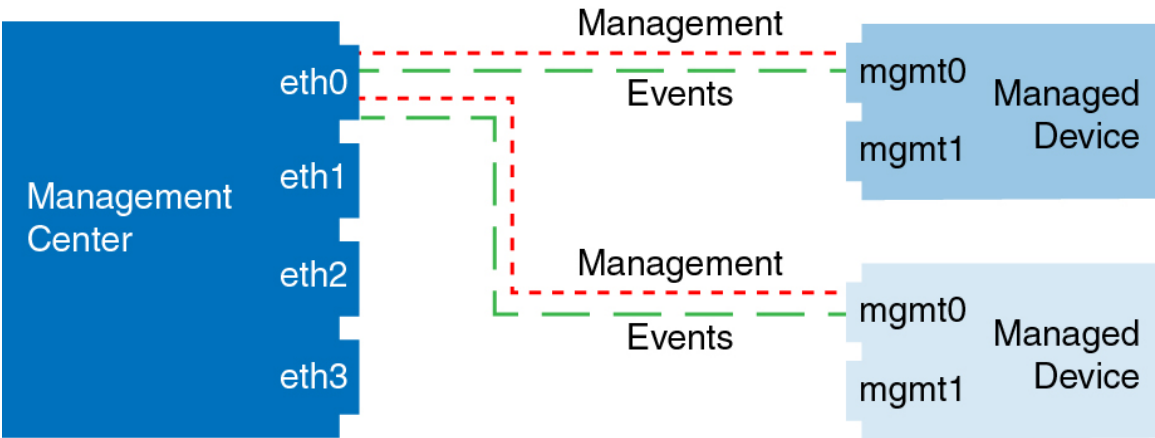
管理和事件流量通道示例



注释 如果在威胁防御上使用数据接口进行管理，则不能对该设备使用单独的管理接口和事件接口。

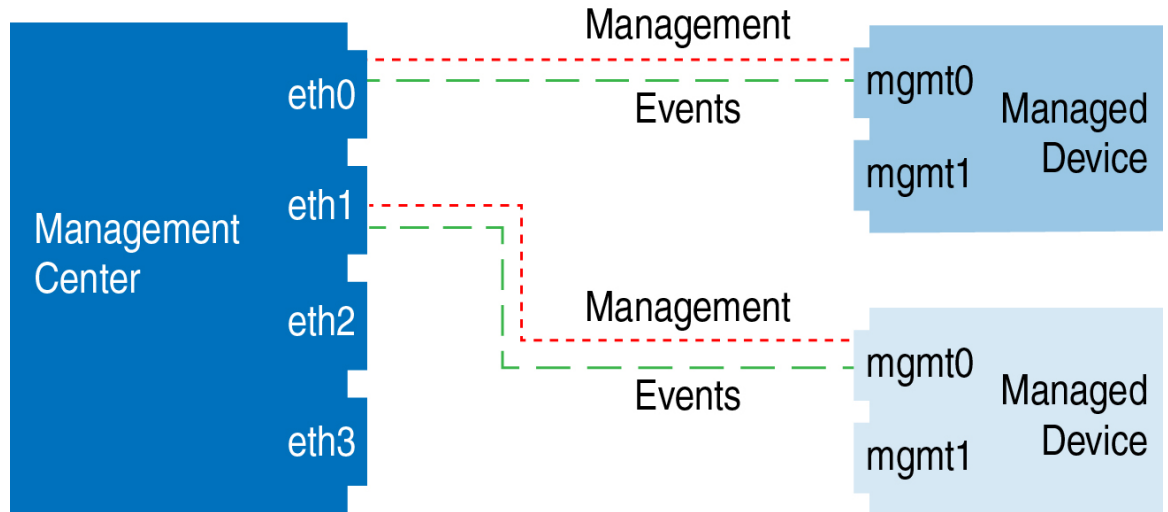
以下示例显示仅使用默认管理接口的管理中心和托管设备。

图 3: Cisco Secure Firewall Management Center 上的单个管理接口



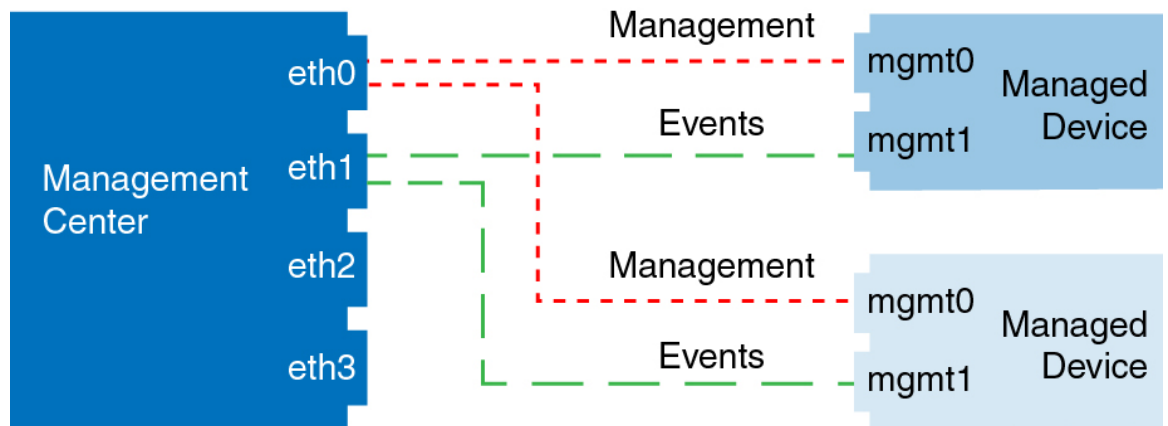
以下示例显示为设备使用单独管理接口的管理中心；每台托管设备均使用 1 管理接口。

图 4: Cisco Secure Firewall Management Center 上的多个管理接口



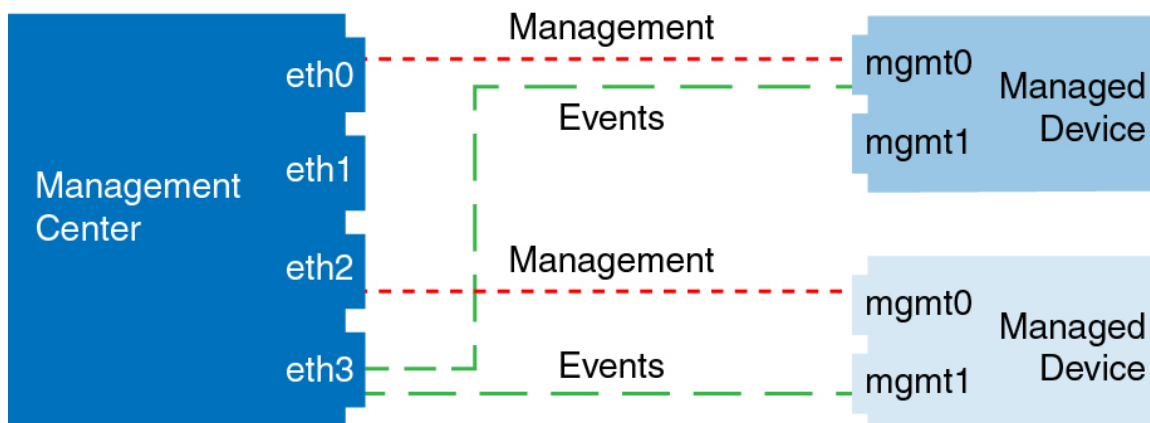
以下示例显示使用单独事件接口的管理中心和托管设备。

图 5: Cisco Secure Firewall Management Center 和托管设备上的单独事件接口



以下示例显示管理中心上多个管理接口与单个事件接口的混合，以及使用单独事件接口或使用单个管理接口的托管设备的混合。

图 6: 混合管理和事件接口用法



设备管理的要求和前提条件

支持的域

设备所在的域。

用户角色

- 管理员
- 网络管理员

管理连接

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。

登录到设备的命令行界面

您可以在威胁防御设备上直接登录命令行界面。如果这是您第一次登录，请使用默认**管理员**用户完成初始设置过程；请参阅[使用 CLI 完成威胁防御初始配置](#)，第 19 页。



注释 当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

- 创建可以使用 **configure user add** 命令登录 CLI 的其他用户账户。

- 如果在连接到控制台端口时出现无法识别的字符，请验证端口设置。如果正确，请使用相同设置的另一台设备尝试使用该电缆。如果电缆正常，您可能需要更换控制台端口的硬件。另请考虑尝试其他工作站以进行连接。

过程

步骤 1 通过控制台端口或使用 SSH 连接至 威胁防御 CLI。

可以通过 SSH 连接到威胁防御设备的管理接口。如果您为 SSH 连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。请参阅 [SSH 访问](#)，以允许与特定数据接口建立 SSH 连接。

对于物理设备，您可以直接连接到设备上的控制台端口。有关控制台电缆的详细信息，请参阅设备的硬件指南。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

控制台端口上的 CLI 是 FXOS（ISA 3000 除外，它是常规 威胁防御 CLI）。使用 威胁防御 CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

对于多实例模式下的机箱，您可以连接到控制台端口上的 FXOS，也可以根据 [配置 SSH 和 SSH 访问列表](#) 为管理接口启用 SSH。默认情况下禁用 SSH。

步骤 2 使用 **admin** 用户名和密码登录。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 3 如果您使用的是控制台端口，请访问 威胁防御 CLI。

connect ftd

多实例模式：

connect ftd name

要查看实例名称，请输入不含名称的命令。

注释

此步骤不适用于 ISA 3000。

示例:

```
firepower# connect ftd
>
```

步骤 4 在 CLI 提示符 (>) 处, 使用命令行访问级别所允许的任何命令。

要返回到控制台端口上的 FXOS, 请输入 **exit**。

步骤 5 (可选) 如果您使用 SSH, 则可以连接到 FXOS。

connect fxos

要返回到 威胁防御 CLI, 请输入 **exit**。

步骤 6 (可选) 访问诊断 CLI:

system support diagnostic-cli

使用此 CLI 可进行高级故障排除。此CLI包括额外 **show** 和其他命令。

此 CLI 有子模式: 用户 EXEC、特权 EXEC 模式。相比用户 EXEC 模式, 在特权 EXEC 模式中, 有更多命令可用。要进入特权 EXEC 模式, 请输入 **enable** 命令; 在收到提示时按 Enter 键, 无需输入密码。

示例:

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

要返回到常规 CLI, 请键入 **Ctrl+a, d**。

为手动注册完成威胁防御初始配置

您可以使用 CLI 完成威胁防御初始配置, 也可以为除 Firepower 4100/9300 之外的所有设备管理器型号完成初始配置。对于 Firepower 4100/9300, 部署逻辑设备时, 完成所有初始配置。请参阅[Firepower 4100/9300上的逻辑设备](#)。

对于零接触调配 (序列号注册), 您不应登录设备或执行初始设置。请参阅[使用序列号添加设备 \(零接触调配\)](#), 第 38 页。

使用设备管理器完成威胁防御初始配置

当您使用 设备管理器 进行初始设置时, 除管理接口和管理器访问设置外, 还会预配置以下接口:

- 以太网 1/1—“外部”, IP 地址来自 DHCP、IPv6 自动配置

- 以太网 1/2（或对于 Firepower 1010 和 Cisco Secure Firewall 1210/1220，为 VLAN1 接口）- “内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

请注意，不会保留其他配置设置，例如访问控制策略或安全区。请注意，诸如内部的 DHCP 服务器、访问控制策略或安全区域等其他设置均未配置。

如果在向管理中心注册之前在设备管理器中执行其他特定于接口的配置，则会保留该配置。

使用 CLI 时，只有管理接口和管理器访问设置会被保留（例如，不保留默认的内部接口配置）。

- Cisco Secure Firewall 4200 不支持 设备管理器。您需要使用 CLI 程序：[使用 CLI 完成威胁防御初始配置，第 19 页](#)
- 此程序不适用于仅将本地 管理中心 部署用于分析的 CDO 托管设备。设备管理器 配置是为了用于配置主管理器。有关配置设备以便进行分析的详细信息，请参阅[使用 CLI 完成威胁防御初始配置，第 19 页](#)。
- 此程序适用于除 Firepower 4100/9300 和 ISA 3000 以外的所有 其他 设备。您可以使用 设备管理器 将这些设备载入管理中心，但由于它们的默认配置不同于其他平台，所以此程序中的详细信息可能会不适用于这些平台。

过程

步骤 1 登录至设备管理器。

a) 在浏览器中输入以下 URL。

- 内部 - <https://192.168.95.1>。
- 管理 - https://management_ip。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。在此过程中，您必须将管理 IP 地址设置为静态地址，因此我们建议您使用内部接口，以免连接被断开。

b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。

c) 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

步骤 2 首次登录设备管理器以完成初始配置时，请使用设置向导。您可以选择通过点击页面底部的跳过设备设置 (Skip device setup) 来跳过安装向导。

完成设置向导后，除了内部接口的默认配置外，您还将拥有外部（以太网 1/1）接口的配置，该接口会在您切换到 管理中心 管理接口时进行维护。

a) 为外部接口和管理接口配置以下选项，然后点击下一步 (Next)。

1. 外部接口地址 (Outside Interface Address) - 此接口通常是互联网网关，并且可用作管理器访问接口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

如果要使用与外部（或内部）不同的接口来进行管理器访问，则必须在完成安装向导后手动配置该接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择关，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 IPv6 - 外部接口的 IPv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

2. 管理接口

如果在 CLI 中执行了初始设置，您将不会看到管理接口设置。

即使您在数据接口上启用管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS (Use OpenDNS)**以重新将合适的 IP 地址载入字段。

防火墙主机名 (Firewall Hostname) - 系统管理地址的主机名。

b) 配置时间设置 (NTP) (Time Setting [NTP]) 并点击下一步 (Next)。

1. 时区 - 选择系统时区。

2. NTP 时间服务器 - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

c) 选择启动 90 日评估期而不注册。

不要向智能软件管理器注册威胁防御；所有许可均在管理中心上执行。

d) 点击完成。

e) 系统将提示您选择**云管理 (Cloud Management)**或**独立 (Standalone)**。对于管理中心管理，请选择**独立 (Standalone)**，然后选择知道了 (Got It)。

步骤 3 （可能需要）配置管理接口。

您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用设备管理器连接的管理接口，则必须重新连接到设备管理器。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。
- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

- 步骤 4** 如果要配置其他接口，包括要用于管理器访问的外部或内部接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。
- 在向管理中心注册设备时，不会保留其他设备管理器配置。
- 步骤 5** 选择**设备 (Device)** > **系统设置 (System Settings)** > **集中管理 (Central Management)**，然后点击**继续 (Proceed)** 以设置管理中心管理。
- 步骤 6** 配置管理中心/CDO 详细信息。

图 7: 管理中心/CDO 详细信息

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

☒ Yes ☐ No

Threat Defense

 10.89.5.16
 fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO

 10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

☐ Data Interface

Please select an interface ▼

☒ Management Interface [View details](#)

CANCEL
CONNECT

- a) 对于是否知道管理中心/CDO 主机名或 IP 地址？，如果您可以使用 IP 地址或主机名访问 管理中心，请点击是，如果 管理中心CDO 位于 NAT 之后或没有公共 IP 地址或主机名，请点击否。

必须至少有一个设备（管理中心或威胁防御设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。

- b) 如果您选择是 (Yes)，则输入管理中心/CDO 主机名或 IP 地址。
- c) 指定管理中心/CDO 注册密钥。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 可用于将多台设备注册到管理中心。

- a) 指定 NAT ID。

此 ID 是您选择的唯一一次性字符串，您还需要在管理中心上指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用 NAT ID，即使它是可选的，但在以下情况下必须使用：

- 您将管理中心 IP 地址设置为 **DONTRESOLVE**。
- 在管理中心上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
- 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
- 管理中心使用多个管理接口。

步骤 7 配置连接配置。

- a) 指定 FTD 主机名。

如果您使用数据接口进行管理中心/CDO 访问接口访问，则此 FQDN 将用于此接口。

- b) 指定 DNS 服务器组。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为管理中心/CDO 访问接口选择数据接口，则此设置会设置数据接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御设备添加到管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御设备同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。

如果要为管理中心/CDO 访问接口/FMC 访问接口选择管理接口，则此设置会配置管理 DNS 服务器。

c) 对于**管理中心/CDO访问接口**，请选择任何已配置的接口。

将威胁防御设备注册到管理中心后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 8 （可选）如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到管理中心之前手动配置默认路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。

步骤 9 （可选）如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保管理中心可接通完全限定域名 (FQDN) 的威胁防御设备。参阅**设备 > 系统设置 > DDNS 服务配置动态 DNS**。

如果您在将威胁防御设备添加到管理中心之前配置 DDNS，则威胁防御设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (<https://help.dyn.com/remote-access-api/>)。

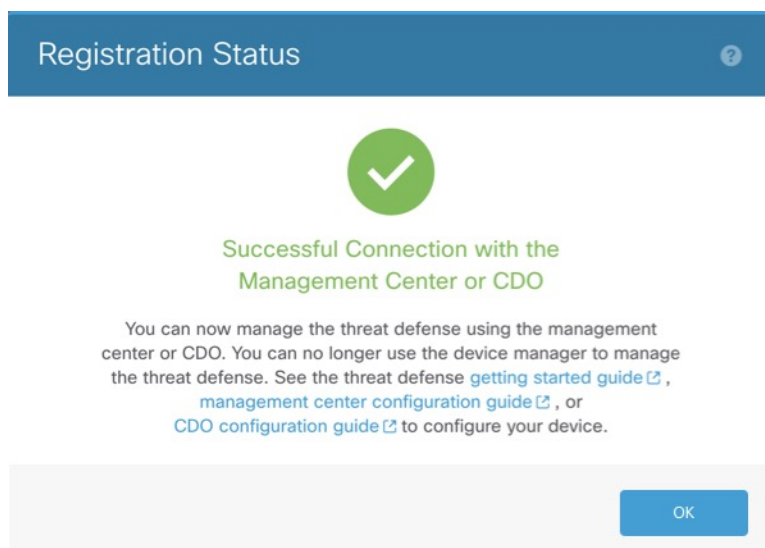
使用管理接口访问管理器时，不支持 DDNS。

步骤 10 点击**连接 (Connect)**。注册状态对话框显示切换到管理中心的当前状态。在**保存管理中心/CDO 注册设置**步骤后，转到管理中心，并添加防火墙。

如果要取消切换到管理中心，请点击**取消注册**。否则，请在**保存管理中心/CDO 注册设置**步骤之后关闭设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果您在**保存管理中心/CDO 注册设置**步骤后保持连接到设备管理器，您最终将看到与**管理中心/CDO 成功连接**对话框。您将断开与设备管理器的连接。

图 8: 成功连接



使用 CLI 完成威胁防御初始配置

连接到威胁防御 CLI 以执行初始设置，包括使用设置向导设置管理 IP 地址、网关和其他基本网络设置。专用管理接口是一种具有自己的网络设置的特殊接口。如果您不想使用管理接口访问管理器，可以使用 CLI 配置数据接口。您还将配置管理中心通信设置。当您使用设备管理器执行初始设置时，如果您切换到管理中心进行管理，除管理接口和管理器访问接口设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略。

此过程适用于除 Firepower 4100/9300 之外的所有模式。要在 Firepower 4100/9300 上部署逻辑设备并完成初始配置，请参阅 [Firepower 4100/9300 上的逻辑设备](#)。

Procedure

步骤 1 从控制台端口连接到威胁防御 CLI，或使用管理接口连接至 SSH，默认情况下其从 DHCP 获取 IP 地址。如果您打算更改网络设置，我们建议使用控制台端口，以免断开连接。

（Firepower 和 Cisco Secure Firewall 硬件型号）控制台端口连接到 FXOS CLI。SSH 会话直接连接到威胁防御 CLI。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

（Firepower 和 Cisco Secure Firewall 硬件型号）在控制台端口，您可以连接到 FXOS CLI。第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

Note

如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。

对于 Firepower 和 Cisco Secure Firewall 硬件，请参阅《[Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 带威胁防御的 Cisco FXOS 故障排除指南](#)》中的[重新映像过程](#)。

对于 ISA 3000，请参阅《[Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南](#)》。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

步骤 3（Firepower 和 Cisco Secure Firewall 硬件型号）如果已连接到控制台端口上的 FXOS，请连接到 威胁防御 CLI。

connect ftd

Example:

```
firepower# connect ftd
>
```

步骤 4 第一次登录威胁防御时，系统会提示您接受《最终用户许可协议》(EULA)和，如果使用 SSH 连接，则会提示您更改 admin 密码。然后，系统将显示 CLI 设置脚本。

Note

除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [威胁防御命令参考](#)。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

Note

即使您在数据接口上启用管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

请参阅以下准则：

- 是否要配置 IPv4？ 和/或 是否要配置 IPv6？ -为至少一种地址类型输入 **y**。
- 输入管理接口的 IPv4 默认网关 和/或 输入管理接口的 IPv6 默认网关-如果要使用数据接口而不是使用管理接口来进行管理器访问，请选择 **手动**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- 输入管理接口的 IPv4 默认网关 和/或 通过 DHCP、路由器或手动方式来配置 IPv6？ - 如果想要使用数据接口而非管理接口进行管理器访问，请将网关设置为 **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。如果要使用管理接口进行管理器访问，应在管理 1/1 网络上设置网关 IP 地址。
- 如果您的网络信息已更改，需要重新连接 - 如果您已建立 SSH 连接，但在初始设置时更改了 IP 地址，连接将断开。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- 本地管理设备？ - 输入 **否** 以使用 管理中心。回答**是**意味着您将改为使用 Cisco Secure Firewall 设备管理器。
- 配置防火墙模式？ - 建议您在初始配置时设置防火墙模式。在初始设置后更改防火墙模式将会清除正在运行的配置。请注意，只有路由防火墙模式支持数据接口管理器访问。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
```

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

```
System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.89.5.1
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```
Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
```

```
Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
- add device configuration
- add network discovery
- add system policy
```

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

>

步骤 5 确定将管理此威胁防御的管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
[display_name]
```

Note

如果您使用 CDO 进行管理，请在此步骤中使用 CDO 生成的 **configure manager add** 命令。

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} - 指定 管理中心 的 FQDN 或 IP 地址。如果 管理中心 不能直接寻址，请使用 **DONTRESOLVE** 并指定 *nat_id*。必须至少有一个设备（管理中心 或 威胁防御）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果在此命令中指定 **DONTRESOLVE**，则 威胁防御 必须有可访问的 IP 地址或主机名。
- *reg_key* - 指定您选择的一次性注册密钥，注册威胁防御时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符（-）。
- *nat_id* - 指定了您选择的唯一一次性字符串，您还需要在注册 威胁防御 时在 管理中心 上指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符（-）。此 ID 不能用于将任何其他设备注册到 管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用 NAT ID，即使它是可选的，但在以下情况下必须使用：
 - 您将 管理中心 IP 地址 设置为 **DONTRESOLVE**。
 - 在 管理中心 上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
 - 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
 - 管理中心 使用多个管理接口。
- *display_name* - 使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 CDO 标识为仅用于分析的主用管理器和本地部署管理中心，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称：
 - *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字）
 - **manager-timestamp**

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Example:

如果管理中心位于 NAT 设备之后，请输入唯一的 NAT ID 以及注册密钥，并指定 **DONTRESOLVE** 而非主机名，例如：

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Example:

如果 威胁防御 位于 NAT 设备之后，请输入唯一的 NAT ID 以及 管理中心 IP 地址或主机名，例如：

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

步骤 6 如果您使用 CDO 作为主要管理器，并希望仅将本地部署管理中心用于分析，请确定本地部署管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
[display_name]
```

Example:

以下示例对具有 CDO 生成的显示名称的 CDO 使用生成的命令，然后仅使用“分析-FMC”显示名称指定用于分析的本地管理中心。

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

步骤 7 (Optional) 配置用于管理器访问的数据接口。

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。

Note

使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

请参阅以下有关使用此命令的详细信息。另请参阅[使用威胁防御数据接口进行管理, on page 4](#)。

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network {ipv4 | ipv6} manual** 命令立即设置它。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您威胁防御添加到管理中心时，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。有关 DNS 服务器配置的详细信息，请参阅下文。在管理中心中，您可以稍后对管理器访问接口配置进行更改，但要确保更改不会阻止威胁防御或管理中心重新建立管理连接。如果管理连接中断，威胁防御将包含 **configure policy rollback** 命令以恢复以前的部署。
- 如果 IP 地址发生变化，DDNS 可确保管理中心访问完全限定域名 (FQDN) 内的威胁防御。如果配置 DDNS 服务器更新 URL，则威胁防御会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便威胁防御可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御添加到管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。

但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在管理中心中手动配置所有这些设置（包括 DNS 服务器），以便与 FTD 配置匹配。

- 将威胁防御注册到管理中心后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

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.
```

>

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
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]:

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 8 (Optional) 限制在特定网络上通过数据接口访问管理器。

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

默认情况下，允许所有网络。

What to do next

将设备注册到 管理中心。

配置事件接口

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，例如，Firepower 4100/9300 和 Cisco Secure Firewall 4200，则可以为仅事件流量启用该接口。

开始之前

要使用单独的事件接口，您还需要在 管理中心 上启用事件接口。请参阅《[Cisco Secure Firewall Management Center 管理指南](#)》。

过程

步骤 1 启用第二个管理接口作为仅事件的接口。

```
configure network management-interface enable management1
```

```
configure network management-interface disable-management-channel management1
```

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。

示例：

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

步骤 2 配置事件接口的 IP 地址。

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。

a) 配置 IPv4 地址：

```
configure network ipv4 manual ip_address netmask gateway_ip management1
```

请注意，此命令中的 *gateway_ip* 用于为设备创建默认路由，因此，您应该输入已经为 *management0* 接口设置的值。它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.

>
```

b) 配置 IPv6 地址：

- 无状态自动配置：

configure network ipv6 router management1

示例：

```
> configure network ipv6 router management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手动配置：

configure network ipv6 manual ip6_address ip6_prefix_length management1

示例：

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

>
```

步骤 3 如果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 management1 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 2](#)，第 25 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）：

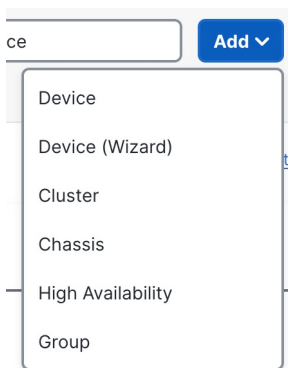
```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination          : 192.168.6.0
Gateway              : 10.10.10.1
Netmask              : 255.255.255.0
[...]
```

管理设备

设备 (Devices) > 设备管理 (Device Management) 页面为您提供一系列信息和选项。

- 查看方式 (View By) - 根据组、许可证、型号、版本或访问控制策略查看设备。
- 设备状态 (Device State) - 根据状态（错误、警告等）查看设备。您可以点击状态图标查看属于它的设备。括号内为各状态所对应的的设备数量。
- 搜索设备 (Search Device) - 按设备名称、主机名或 IP 地址搜索设备。
- 添加 (Add) - 添加设备和其他可管理组件。

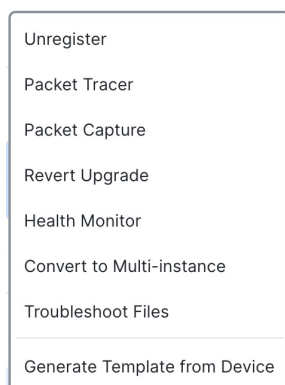
图 9: 添加菜单



- 列 - 点击列标题可按该列进行排序。
 - 名称
 - 型号
 - 版本

- **机箱 (Chassis)** - 对于支持的型号，点击**管理 (Manage)** 以显示集成机箱管理器。对于 Firepower 4100/9300，该链路会交叉启动 机箱管理器。
- **许可证**
- **访问控制策略 (Access Control Policy)** - 点击访问控制策略列中的链接以查看部署到设备的策略。
- **自动回滚 (Auto-Rollback)** - 显示在部署导致管理连接中断时，配置的自动回滚是启用 (🔄) 还是禁用 (🔒)。请参阅[编辑部署设置](#)。
- **编辑 (Edit)** - 对于每个设备，使用 **编辑 (🔗)** 图标编辑设备设置。
您也可以点击设备名称或 IP 地址。
- **更多 (More)** - 对于每个设备，点击 **更多 (⋮)** 图标以执行其他操作：

图 10: 更多菜单



- **取消注册**-取消注册设备。
- **数据包跟踪器 (Packet Tracer)** - 导航至数据包跟踪器页面，以便通过将模型数据包注入系统来检查设备上的策略配置。
- **数据包捕获 (Packet Capture)** - 导航至数据包捕获页面，您可以在其中查看系统在处理数据包时所采取的判定和操作。
- **恢复升级 (Revert Upgrade)** - 恢复上次升级后所做的升级和配置更改。此操作会将设备恢复到升级前的版本。
- **运行状况监控器 (Health Monitor)** - 导航至设备的运行状况监控页面。
- **转换为多实例 (Convert to Multi-instance)** - 对于支持的型号，将机箱转换为多实例模式。
- **故障排除文件 (Troubleshooting Files)** - 生成故障排除文件，您可以在其中选择要在报告中包含的数据类型。
- **从设备生成模板 (Generate Template from Device)** - 从已注册的设备生成新的设备模板。新模板的配置与生成模板的设备相同。您可以从独立设备和 HA 设备生成新的设备模板。但是，如果从 HA 设备生成模板，新模板将不包含故障转移配置。

添加设备组

管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。您可以展开和折叠组中的设备列表。

如果将高可用性对中的主设备添加到某个组，则系统会将两台设备均添加到该组中。如果取消高可用性，则两台设备均会保留在该组中。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 从添加 (Add) 下拉菜单中，选择添加组 (Add Group)。

要编辑现有的组，请点击要编辑的组的 编辑 (✎)。

步骤 3 输入 **Name**。

步骤 4 在可用设备 (Available Devices) 下，选择一台或多台要添加到设备组的设备。点击的同时使用 Ctrl 或 Shift 选择多台设备。

步骤 5 点击添加 (Add) 将所选设备包含在设备组中。

步骤 6 或者，要将设备从设备组中删除，请点击要删除的设备旁边的 删除 (🗑)。

步骤 7 点击确定 (OK) 以添加组。

向管理中心注册

管理中心 提供多种设备注册方法。

注册密钥方法

使用您在管理中心和设备初始配置中指定的注册密钥来添加设备。

使用注册密钥添加设备

按照此程序使用注册密钥将单个设备添加到 管理中心。如果您计划链接设备以实现高可用性，则仍必须使用此程序；请参阅[添加高可用性对](#)。有关集群，请参阅您的型号的集群章节。

您还可以使用此程序添加由 云交付的防火墙管理中心管理的设备，并且您希望仅将本地 管理中心部署用于事件日志记录和分析目的。

使用模板以添加设备，请参阅[使用注册密钥添加设备-设备模板](#)，第 33 页。

如果使用 管理中心 高可用性，请 仅 将设备添加到活动 管理中心。注册到主用 管理中心的设备将自动注册到备用设备。

开始之前

- 将设备设置为由 管理中心管理。请参阅：
 - [为手动注册完成威胁防御初始配置，第 12 页](#)
 - 《适用于您的型号的入门指南》
- 管理中心必须注册到智能软件管理器。有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须取消注册并该设备。

过程

步骤 1 选择 **设备 > 设备管理**。

步骤 2 从 **添加** 下拉菜单中，选择 **设备**。

图 11: 使用注册密钥添加设备

Add Device ?

☐ CDO Managed Device

Host:

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

☒ Carrier
☒ Malware Defense
☒ IPS
☒ URL

Advanced

Unique NAT ID:

☒ Transfer Packets

Cancel Register

步骤 3 如果要将云托管设备添加到本地部署 管理中心 仅用于分析，请选中**CDO 托管设备**。
系统会隐藏许可和数据包传输设置，因为它们由 CDO（前称 CDO）管理。您可以跳过这些步骤。

图 12: 为 CDO 添加设备

Add Device ⓘ

☒ CDO Managed Device

Host:
10.89.5.41

Display Name:
3110-1

Registration Key:*
....

Group:
None

Advanced

Unique NAT ID:
31101

Transfer Packets is configured in CDO

[Cancel](#) [Register](#)

步骤 4 对于主机，输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。

如果您将此字段留空，则设备上的初始配置需要包括可访问的 管理中心 IP 地址或主机名以及 NAT ID。有关详细信息，请参阅[NAT 环境，第 6 页](#)。

步骤 5 对于显示名称 (Display Name)，输入要在 管理中心 中显示的设备名称。之后将无法更改该名称。

步骤 6 对于注册密钥 (Registration Key)，输入您在初始配置中相同的注册密钥。注册密钥是一个一次性的共享密钥。密钥最多 37 个字符，包括字母数字 (A - Z、a - z、0 - 9) 和连字符 (-)。不需要每台设备的注册密钥都是唯一的。

步骤 7 （可选）将设备添加到设备 组。

步骤 8 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。

如果设备与所选策略不兼容，部署会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。请在解决导致失败的问题后，手动将配置部署到设备。

步骤 9 选择要应用到设备的许可证。

在添加设备后，您可以从系统 (System) > 许可证 (Licenses) > 智能许可证 (Smart Licenses) 页面应用许可证。

对于 threat defense virtual，您还必须选择性能层 (Performance Tier)。选择与您账户中的许可证相匹配的级别很重要。在选择级别之前，您的设备默认为 FTDv50 选项。有关可用于 threat defense virtual

的性能分层许可证授权的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 *FTDv* 许可证。

注释

如果要将在 threat defense virtual 升级到 7.0+ 版，可以选择 **FTDv - 变量 (FTDv - Variable)** 来保持当前的许可证合规性。

步骤 10 如果在初始化配置中指定了 NAT ID，在高级 (**Advanced**) 部分中，在**唯一 NAT ID (Unique NAT ID)** 中输入相同的 NAT ID。

唯一 NAT ID 指定您选择的唯一的一次性字符串，您也可以在初始设置时在设备上指定该字符串。当一端未指定可访问的 IP 地址或主机名时（例如，如果您将**主机 (Host)** 字段留空），则需要填写。虽然在技术上是可选的，但我们建议始终指定 NAT ID，因为它在某些情况下是必需的，即使您知道两端的 IP 地址也是如此。ID 最多 37 个字符，包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。

步骤 11 选中**传输数据包 (Transfer Packets)** 复选框，以便对于每个入侵事件，设备将数据包传输到管理中心进行检查。

默认情况下，此选项已启用。对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到管理中心进行检查。如果禁用此选项，则只会向管理中心发送事件信息，而不会发送数据包。

步骤 12 点击 **Register**。

管理中心可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果设备注册失败，请检查以下项：

- Ping - 访问设备 CLI，然后使用以下命令 ping 管理中心 IP 地址：

```
ping system ip_address
```

如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改设备 IP 地址，使用 **configure network {ipv4 | ipv6} manual** 命令。

- 注册密钥、NAT ID 和管理中心 IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在设备上使用 **configure manager add** 命令设定注册密钥和 NAT ID。

有关更多故障排除信息，请参阅 <https://cisco.com/go/fmc-reg-error>。

使用注册密钥添加设备-设备模板

您可以使用模板添加设备，向管理中心注册设备，并使用所给模板配置来调出设备。

开始之前

按照[使用设备模板进行设备管理](#)创建设备模板。您必须为每个设备指定所需的变量和网络对象覆盖，并确保为目标设备模型进行了模型映射。

建议您创建核对表，以确保在设备上应用模板之前已正确输入模板中的所有配置。

核对表示例如下所示。

- 检查版本、型号、操作模式。
- 检查变量和覆盖列表。
- 检查变量和覆盖值的健全性。
- 检查是否存在所需的模型映射。
- 检查并行设备模板操作是否正在进行。



注释 如果要添加将由数据接口管理的设备，请确保配置的模板与设备的连接参数兼容。有关详细信息，请参阅[为通过数据接口管理的威胁防御设备配置模板](#)。

过程

- 步骤 1** 选择设备 > 设备管理。
- 步骤 2** 从添加 (Add) 下拉菜单中，选择设备（向导）(Device [Wizard])。
- 步骤 3** 点击注册密钥 (Registration Key)，然后点击下一步 (Next)。

图 13: 设备注册方法

- 步骤 4** 在多域环境中，从下拉列表中选择域 (Domain)，然后点击下一步 (Next)。

图 14: 域

The screenshot shows a multi-step wizard titled "Add Device(s)". The steps are listed on the left: 1. Device registration method, 2. Domain, 3. Initial device configuration, and 4. Device details. Step 2, "Domain", is the current active step. It contains a label "Domain *" and a dropdown menu with "Global/Pubs" selected. To the right of the dropdown are "Previous" and "Next" buttons. At the bottom right of the wizard are "Cancel" and "Add Device" buttons.

Add Device(s)

1 Device registration method

Device registration method **Registration Key**

2 **Domain**

Domain *

Global/Pubs

3 Initial device configuration

4 Device details

Previous Next

Cancel Add Device

步骤 5 在初始设备配置 (Initial device configuration) 中，从设备模板 (Device template) 下拉列表中选择模板。

图 15: 初始设备配置

Add Device(s)

1

Device registration method

Device registration method **Registration Key**

2

Domain

Domain **Global/Pubs**

3

Initial device configuration

Device template *

inside-outside-dmz

Device models supported for the selected template

Firepower 1010 Threat Defense

Access control policy : acp1

This template requires devices to be managed using the Management interface. Ensure that the device's connection to Management Center is from the Management interface.

4

Device details

Previous

Next

Cancel

Add Device

步骤 6 指定设备详细信息。

图 16: 设备详细信息

Add Device(s)

1

Device registration method

Device registration method **Registration Key**

2

Domain

Domain **Global/Pubs**

3

Initial device configuration

Device template **inside-outside-dmz**

4

Device details

Host

10.89.5.6

Display name *

1120-1

Registration key *

....

Device group

Select...

Unique NAT ID

11201

Note: Either Host or NAT ID is required.

Variables

Variables	Value
\$outside_ip	209.165.200.228/27 (IPv4 Network; Example: 209.165.200.224/27)

Previous

Cancel Add Device

- a) 对于**主机**，输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。

如果您将此字段留空，则设备上的初始配置需要包括可访问的 管理中心 IP 地址或主机名以及 NAT ID。有关详细信息，请参阅[NAT 环境，第 6 页](#)。

- b) 对于**显示名称 (Display name)**，输入要在管理中心中显示的设备名称。之后将无法更改该名称。
- c) 对于**注册密钥 (Registration Key)**，输入您在初始配置中相同的注册密钥。注册密钥是一个一次性的共享密钥。密钥最多37个字符，包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。不需要每台设备的注册密钥都是唯一的。
- d) （可选）将设备添加到**设备组**
- e) 如果在初始配置期间已指定 NAT ID，请为**唯一 NAT ID**输入相同的 NAT ID。

唯一 NAT ID 指定您选择的唯一的一次性字符串，您也可以在初始设置时在设备上指定该字符串。当一端未指定可访问的 IP 地址或主机名时（例如，如果您将**主机 (Host)** 字段留空），则需要填写。虽然在技术上是可选的，但我们建议始终指定 NAT ID，因为它在某些情况下是必需

的，即使您知道两端的 IP 地址也是如此。ID 最多 37 个字符，包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到 管理中心。

- f) 选中**传输数据包 (Transfer Packets)** 复选框，以便对于每个入侵事件，设备将数据包传输到 管理中心 进行检查。

对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到 管理中心 进行检查。如果禁用此选项，则只会向 管理中心 发送事件信息，而不会发送数据包。

- g) 输入变量和网络对象覆盖的值。

步骤 7 点击**添加设备 (Add Device)** 以启动设备注册。向 管理中心 成功注册设备后，系统将应用模板配置。

序列号方法（零接触调配）

通过零接触调配，您可以按序列号将设备注册到 管理中心，而无需在设备上执行任何初始设置。

使用序列号添加设备（零接触调配）

通过零接触调配，您可以按序列号将设备注册到 管理中心，而无需在设备上执行任何初始设置。管理中心 与思科安全云和 CDO 集成以实现此功能。

使用 零接触调配时，系统会预配置以下接口：请注意，不会保留其他配置设置，例如访问控制策略或安全区。请注意，诸如内部的 DHCP 服务器、访问控制策略或安全区域等其他设置均未配置。

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 Firepower 1010 和 Cisco Secure Firewall 1210/1220，为 VLAN1 接口）- “内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

按照此程序使用基本配置将单个设备添加到 管理中心。要使用模板添加一个或多个设备，请参阅[使用序列号来添加设备（零接触调配）- 设备模板，第 43 页](#)。

零接触调配 不支持集群或多实例模式。

仅当使用管理接口时才支持高可用性，因为 零接触调配 使用 DHCP，数据接口和高可用性不支持 DHCP。

零接触调配 仅在以下运行 7.2 和 7.4 或更高版本的型号上受支持；在 7.2.4 之前的版本中，管理中心 必须可公开访问。

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（在支持的版本上）
- Cisco Secure Firewall 3100

开始之前

- 确保设备已取消配置或全新安装。零接触调配仅适用于新设备。预配置可以禁用 零接触调配，具体取决于您配置设备的方式。
- 连接外部接口或管理接口，使其能够访问互联网。如果您使用外部接口进行零接触调配，请勿同时连接管理接口；如果管理接口从 DHCP 获取 IP 地址，则外部接口的路由将不正确。
- 如果设备没有公共 IP 地址或 FQDN，或者您使用管理接口，请为 管理中心 设置公共 IP 地址/FQDN（例如，如果它在 NAT 之后），以便设备可以发起管理连接。请参阅 **系统 (System) > 配置 (Configuration) > 管理器远程访问 (Manager Remote Access)**。
- 管理中心必须注册到智能软件管理器。有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须取消注册并该设备。

过程

步骤 1 首次使用序列号添加设备时，请将 管理中心 与思科安全云集成。

注释

对于 管理中心 高可用性对，您还需要将辅助 管理中心 与思科安全云集成。

- a) 选择**集成 (Integration) > 思科安全云 (Cisco Security Cloud)**。
- b) 点击 **启用思科安全云 (Enable Cisco Security Cloud)** 打开单独的浏览器选项卡，让您登录思科安全云账户并确认显示的代码。

确保此页面未被弹出窗口阻止程序阻止。如果您还没有思科安全云和 CDO 账户，您可以在程序期间添加一个。

有关此集成的详细信息，请参阅 [《Cisco Secure Firewall Management Center 管理指南》](#) 中的“系统配置”一章。

CDO 会在您将 管理中心 与思科安全云集成后载入本地 管理中心。CDO 需要在其清单中添加 管理中心，以便进行零接触调配。但是，您不需要直接使用 CDO。如果您使用 CDO，其 管理中心 支持仅限于设备载入、查看其托管设备、查看与管理中心关联的对象，以及交叉启动管理中心。

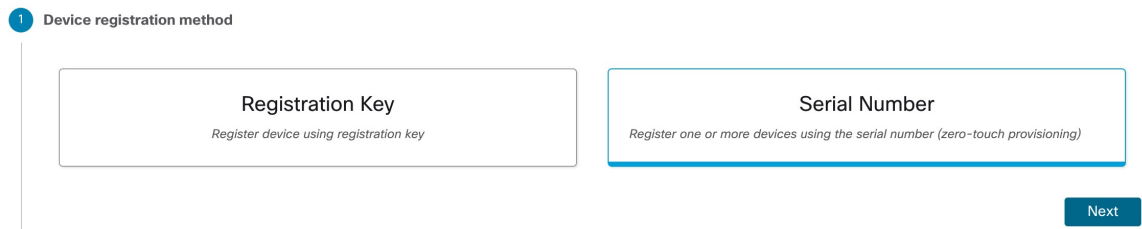
- c) 确保选中**启用零接触调配 (Enable Zero-Touch Provisioning)**。
- d) 点击**保存 (Save)**。

步骤 2 选择**设备 > 设备管理**。

步骤 3 从添加 (**Add**) 下拉菜单中，选择**设备（向导） (Device [Wizard])**。

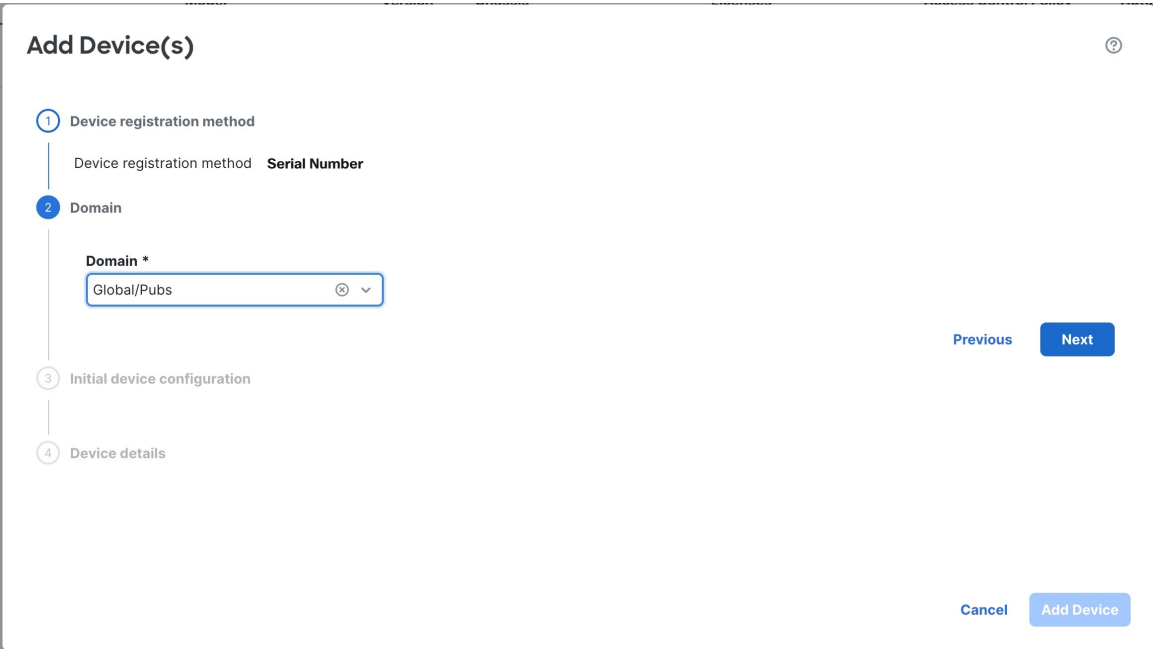
步骤 4 点击**使用序列号 (Use Serial Number)**，然后点击**下一步 (Next)**。

图 17: 设备注册方法



步骤 5 在多域环境中，从下拉列表中选择域 (Domain)，然后点击下一步 (Next)。

图 18: 域



步骤 6 对于初始设备配置 (Initial device configuration)，点击基本 (Basic) 单选按钮。

图 19: 初始设备配置方法

Add Device (Wizard)

1 Device registration method
Device registration method **Serial Number**

2 Management Center Role
Management **Primary manager**

3 Initial device configuration

Choose initial device configuration method

☒ Basic ☐ Device template

Apply basic configuration, including the access control policy.

Access Control Policy *

wfx_automatio...

Smart licensing

Performance tier (threat defense virtual only)

FTDv50 - 10 Gbps

☒ Carrier

☒ Malware Defense

☒ IPS

☒ URL Filtering

Ensure that your smart licensing account has the required licenses.

☒ Transfer packet data as well as event data to the management center for inspection.

Previous **Next**

4 Device details

Cancel **Add Device**

- a) 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。

如果设备与所选策略不兼容，部署会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。请在解决导致失败的问题后，手动将配置部署到设备。

- b) 选择要应用到设备的智能许可许可证。

在添加设备后，您可以从系统 (**System**) > 许可证 (**Licenses**) > 智能许可证 (**Smart Licenses**) 页面应用许可证。

- c) 点击下一步 (**Next**)。

步骤 7 配置设备详细信息 (**Device details**)。

图 20: 设备详细信息

Add Device

1 Device registration method
Device registration method **Serial Number**

2 Initial device configuration
Access control policy **wfx_automationPolicy123**

3 Device details

Configure the public IP address or FQDN for the Management Center, except in scenarios where the Threat Defense device is publicly reachable, running a version earlier than 7.4, and is connected to the data interface. To configure the public IP address or FQDN, go to [Configuration > Manager Remote Access](#).

Serial number Display name

Device group

Set the device password
Enter a new password if you have not previously changed the device's default password.

New password Confirm password

Skip this field if you already changed the password on the device. If you provide a new password in this case, registration will fail.

[Previous](#)

[Cancel](#) [Add Device](#)

- 输入序列号。
- 输入要在 管理中心 中显示的显示名称
- （可选）选择设备组 (Device Group)。
- 设置设备密码。

如果此设备未配置或全新安装，则需要设置新密码。如果您已登录并更改了密码，请将此字段留空。否则，注册将失败。

步骤 8 点击添加设备。

管理中心可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。

在外部接口上使用零接触调配时，CDO 会充当 DDNS 提供商并执行以下操作：

- 使用仅限 **FMC (FMC Only)** 方法在外部启用 DDNS。此方法仅支持零接触调配设备。
- 使用以下主机名映射外部 IP 地址：**serial-number.local**。
- 提供到 管理中心 的 IP 地址/主机名映射，以便将主机名解析为正确的 IP 地址。
- 如果 IP 地址发生变化（例如 DHCP 租用更新），则会向 管理中心 发送通知。

如果在管理接口上使用零接触调配，则不支持 DDNS。管理中心 必须可公开访问，以便设备能够发起管理连接。

您可以继续使用 CDO 作为 DDNS 提供商，也可以稍后将 管理中心 中的 DDNS 配置更改为其他方法。有关详细信息，请参阅[配置动态 DNS](#)。

如果设备注册失败，请参阅[解决序列号（零接触调配）注册问题](#)，第 52 页。

使用序列号来添加设备（零接触调配）- 设备模板

通过零接触调配，您可以按序列号将设备注册到 管理中心，而无需在设备上执行任何初始设置。管理中心 与 思科安全云 和 CDO 集成以实现此功能。

您可以使用模板添加设备，向 管理中心 注册设备，并使用模板配置来调出设备。

使用此程序可使用序列号和设备模板将设备添加到 管理中心。要添加设备而不使用模板，请参阅[使用序列号添加设备（零接触调配）](#)，第 38 页。

零接触调配 不支持集群或多实例模式。

仅当使用管理接口时才支持高可用性，因为 零接触调配 使用 DHCP，数据接口和高可用性不支持 DHCP。

以下运行 7.4 或更高版本的型号支持零接触调配：

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（在支持的版本上）
- Cisco Secure Firewall 3100

开始之前

- 确保设备已取消配置或全新安装。零接触调配仅适用于新设备。预配置可以禁用 零接触调配，具体取决于您配置设备的方式。
- 连接外部接口或管理接口，使其能够访问互联网。如果您使用外部接口进行零接触调配，请勿同时连接管理接口；如果管理接口从 DHCP 获取 IP 地址，则外部接口的路由将不正确。
- 如果设备没有公共 IP 地址或 FQDN，或者您使用管理接口，请为 管理中心 设置公共 IP 地址/FQDN（例如，如果它在 NAT 之后），以便设备可以发起管理连接。请参阅 **系统 (System) > 配置 (Configuration) > 管理器远程访问 (Manager Remote Access)**。
- 管理中心必须注册到智能软件管理器。有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须取消注册并该设备。
- 按照[使用设备模板进行设备管理](#)创建设备模板。您必须为每个设备指定所需的变量和网络-对象覆盖，并确保为目标设备模型进行了模型映射。

建议您创建核对表，以确保在设备上应用模板之前已正确输入模板中的所有配置。

核对表示例如下所示。

- 检查版本、型号、操作模式。
- 检查变量和覆盖列表。
- 检查变量和覆盖值的健全性。
- 检查是否存在所需的模型映射。
- 检查并行设备模板操作是否正在进行。



注释 如果要添加将由数据接口管理的设备，请确保配置的模板与设备的连接参数兼容。有关详细信息，请参阅[为通过数据接口管理的威胁防御设备配置模板](#)。

过程

步骤 1 首次使用序列号添加设备时，请将 管理中心 与思科安全云集成。

注释

对于 管理中心 高可用性对，您还需要将辅助 管理中心 与思科安全云集成。

- a) 选择集成 (**Integration**) > 思科安全云 (**Cisco Security Cloud**)。
- b) 点击 **启用思科安全云 (Enable Cisco Security Cloud)** 打开单独的浏览器选项卡，让您登录思科安全云账户并确认显示的代码。

确保此页面未被弹出窗口阻止程序阻止。如果您还没有思科安全云和 CDO 账户，您可以在程序期间添加一个。

有关此集成的详细信息，请参阅 [《Cisco Secure Firewall Management Center 管理指南》](#) 中的“系统配置”一章。

CDO 会在您将 管理中心 与思科安全云集成后载入本地 管理中心。CDO 需要在其清单中添加 管理中心，以便进行零接触调配。但是，您不需要直接使用 CDO。如果您使用 CDO，其 管理中心 支持仅限于设备载入、查看其托管设备、查看与 管理中心 关联的对象，以及交叉启动 管理中心。

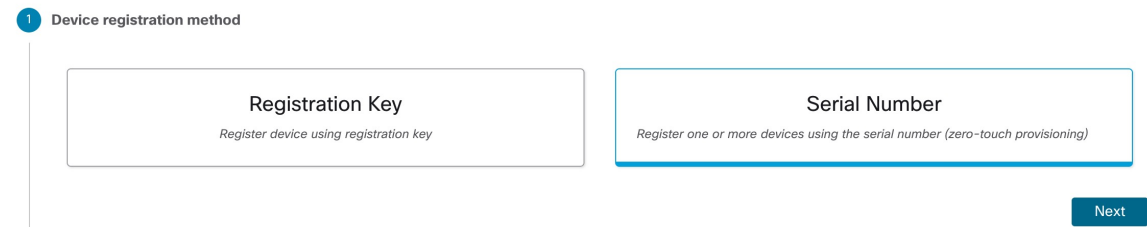
- c) 确保选中 **启用零接触调配 (Enable Zero-Touch Provisioning)**。
- d) 点击 **保存 (Save)**。

步骤 2 选择设备 > 设备管理。

步骤 3 从添加 (**Add**) 下拉菜单中，选择设备（向导）(**Device [Wizard]**)。

步骤 4 点击使用序列号 (**Use Serial Number**)，然后点击下一步 (**Next**)。

图 21: 设备注册方法



1 Device registration method

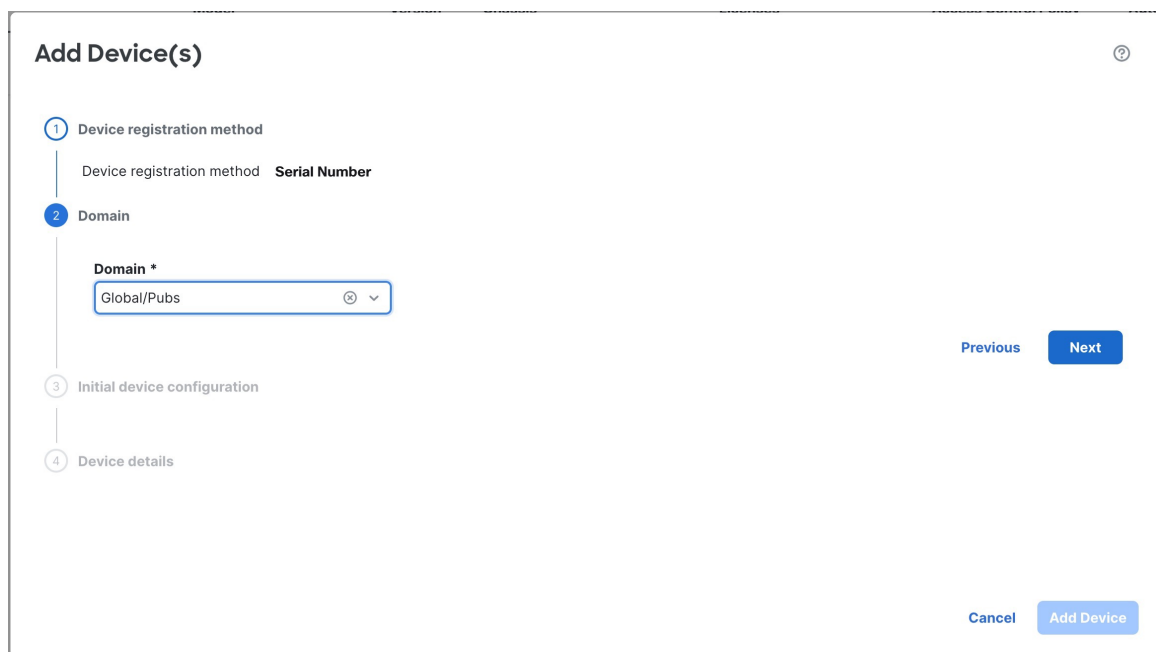
Registration Key
Register device using registration key

Serial Number
Register one or more devices using the serial number (zero-touch provisioning)

Next

步骤 5 在多域环境中，从下拉列表中选择域 (**Domain**)，然后点击下一步 (**Next**)。

图 22: 域



Add Device(s)

1 Device registration method

Device registration method **Serial Number**

2 Domain

Domain *

Global/Pubs

3 Initial device configuration

4 Device details

Previous Next

Cancel Add Device

步骤 6 对于初始设备配置 (**Initial device configuration**)，点击设备模板 (**Device template**) 单选按钮。

图 23: 初始设备配置

Add Device (Wizard) ?

1 Device registration method

Device registration method **Serial Number**

2 Initial device configuration

Choose initial device configuration method

☐ Basic ☒ Device template

Preconfigure settings using a template. A template is applied on a device after registration only if the device model and version support template application. If not, the template is not applied, and the initial deployment is skipped. For more information, see the [Online Help](#).

Device template *

1010-template

Access control policy : wfx_automationPolicy123

Device models supported for the selected template

- ☒ Firepower 1010 Threat Defense

Warning: This template requires devices to be managed using the Management interface. Ensure that the device's connection to Management Center is from the Management interface.

3 Device details

[Previous](#) [Next](#)

[Cancel](#) [Add Device](#)

步骤 7 在下拉列表中，选择设备模板 (**Device template**)，然后点击下一步 (**Next**)。

步骤 8 在设备详细信息 (**Device details**) 中，上传包含模板所需的设备详细信息的 CSV 文件。

图 24: 设备详细信息

Add Device (Wizard)

1

Device registration method

Device registration method **Serial Number**

2

Initial device configuration

Device template **1010-template**

3

Device details

Configure the public IP address or FQDN for the Management Center, except in scenarios where the Threat Defense device is publicly reachable, running a version earlier than 7.4, and is connected to the data interface. To configure the public IP address or FQDN, go to [Configuration > Manager Remote Access](#).

CSV sample template file: [SampleTemplate.csv](#)

You can onboard multiple Threat Defense devices by uploading a properly formatted .csv file containing the following information for each of these devices:

Display Name (Type: String; Example: Branch01Firewall)

Serial Number (Type: String; Example: JADX345670EG)

Device Group (Type: String; Example: testgroup)

Admin Password (Type: String; Example: E28@20iUrhx)

Variables
Variables are defined in the template and mentioned in sample.csv in the format \$<varName>.

\$WANLinkIP (Type: IPv4 Network; Example: 209.165.200.224/27)

Network Object Overrides
In the template, network objects are defined to be overridden on the target devices and are mentioned in sample.csv in the format <objType>:<objName> .

Host:gateway (Type: Host; Example: IPv4-209.165.200.225, IPv6-2001:DB8::1)

Filename:

SampleTemplate.csv

Browse

All entries are validated successfully.

Cancel

Add Device

- 下载 **SampleTemplate.csv**。此文件包含您需要为每台设备定义的值的的所有必需报头。有关 CSV 模板文件字段的详细信息，请参阅 [使用设备模板注册序列号的 CSV 模板文件](#)。
- 拖放 CSV 模板文件或浏览选择要上传的 CSV 模板文件。系统会在上传文件后进行验证检查。
CSV 模板文件上传成功后，CSV 模板文件的内容将以表格格式显示。

步骤 9 点击添加设备 (Add Device) 以注册设备。

在外部接口上使用零接触调配时，CDO 会充当 DDNS 提供商并执行以下操作：

- 使用 "fmcOnly" 方法在外部启用 DDNS。此方法仅支持零接触调配设备。

- 使用以下主机名映射外部 IP 地址：*serial-number.local*。
- 提供到 管理中心 的 IP 地址/主机名映射，以便将主机名解析为正确的 IP 地址。
- 如果 IP 地址发生变化（例如 DHCP 租用更新），则会向 管理中心 发送通知。

如果在管理接口上使用零接触调配，则不支持 DDNS。管理中心 必须可公开访问，以便设备能够发起管理连接。

您可以继续使用 CDO 作为 DDNS 提供商，也可以稍后将 管理中心 中的 DDNS 配置更改为其他方法。有关详细信息，请参阅[配置动态 DNS](#)。

如果设备注册失败，请参阅[解决序列号（零接触调配）注册问题](#)，第 52 页。

使用设备模板注册序列号的 CSV 模板文件

CSV 模板文件的大小必须小于 2 MB。文件名必须满足以下条件：

- 最多可包含 64 个字符。
- 只允许使用字母数字字符和特殊字符，如破折号 (-)、句点 (.) 和下划线 (_)。
- 不得包含任何空格。

包含两个设备配置的 CSV 模板文件示例如下。

```
DisplayName,SerialNumber,AdminPassword,$WANLinkIP,Host:gateway
Branch A FTD,JADX345410AB,C15c05n0rt#,10.20.30.1/24,10.2.3.1
Branch B FTD,JADX345670CE,Admin123!,10.20.30.5/24,10.2.3.1
```

格式正确的 CSV 文件包含以下字段。

必填字段

- **DisplayName**— 设备的名称。类型：字符串。示例：test1
- **SerialNumber** - 设备的序列号。类型：字符串，示例：JADX345670EG
- **AdminPassword** - 用于管理员访问的密码，类型：字符串，示例：E28@2OiUrhx

可选字段

- **DeviceGroup** - 设备组的名称，类型：字符串，示例：testgroup

变量

使用以下格式：*\$varName*。

变量示例：**\$LAN-Devices-IPv4Address** - LAN 设备的 IPv4 地址。类型：字符串。示例：10.2.3.4/24。

网络对象覆盖

使用以下格式：*objType:objName*。

网络对象覆盖示例：**Network:LAN-Devices-Network-** LAN 设备网络的 IP 地址。类型：字符串。示例：10.2.3.0/24

FQDNs

对于序列号注册，会自动启用 DDNS。如果要为 **仅 FMC** 类型 DDNS 设置与默认值不同的值，则可以在模板中配置设置。在此情况下，为 *hostname* 提供 CSV 值时，请务必将其指定为 *serialnumber.local*。

添加机箱

您可以将 Firepower 4100/9300 添加到管理中心。管理中心和机箱使用机箱 MGMT 接口共享单独的管理连接。管理中心提供机箱级运行状况警报。对于配置，您仍需要使用 Cisco Secure Firewall 机箱管理器或 FXOS CLI。



注释 对于 Cisco Secure Firewall 3100/4200，机箱会作为多实例模式的一部分被添加到管理中心。请参阅 [将设备转换为多实例模式](#)。但是，如果您使用 CLI 转换为多实例模式 ([在 CLI 启用多实例模式](#))，请跳至此程序的 [步骤 3，第 50 页](#) 以便将机箱添加到管理中心。

过程

步骤 1 通过控制台端口或使用 SSH 连接至机箱 FXOS CLI。

步骤 2 配置管理中心。

```
create device-manager manager_name [hostname {hostname | ipv4_address | ipv6_address}] [nat-id nat_id]
```

系统将提示您输入注册密钥。

您可以从任何范围输入此命令。无需使用 **commit-buffer** 即可立即接受此命令。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the 管理中心。必须至少有一个设备（管理中心或机箱）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果未在此命令中指定 **hostname**，则机箱必须具有可访问的 IP 地址或主机名，并且必须指定 **nat-id**。
- **nat-id** *nat_id*- 指定您选择的唯一的一次性字符串，注册机箱时若一方没有指定可访问的 IP 地址或主机名，则也要在 管理中心 机箱上指定它。如果您不指定 **hostname**，则必须设置，但我们建议您始终设置 NAT ID，即使您指定了主机名或 IP 地址。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。

- **Registration Key:** *reg_key*- 系统将提示您输入选择的一次性注册密钥，注册机箱时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。

示例:

```
firepower# create device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

步骤 3 在管理中心中，使用机箱管理 IP 地址或主机名添加机箱。

- 选择 **设备 > 设备管理**，然后选择 **添加 > 添加集群**。

图 25: 添加机箱

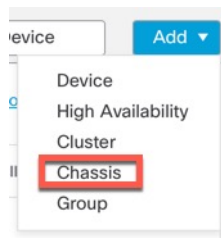


图 26: 添加机箱

Add Chassis

ⓘ This operation is only supported on 3100, 4100 & 9300 chassis

Hostname/IP Address†

10.89.5.9

Chassis name

eng1

Registration key*

....

Device Group

Select...

Unique NAT ID†

winchester

† Either host or NAT ID is required.

Cancel Submit

- 在 **主机/IP 地址** 字段中，输入要添加的设备的 IP 地址或主机名。

如果您不知道主机名或 IP 地址，可以将此字段留空，指定**唯一 NAT ID**。

- c) 在**机箱名称**字段中，输入要在 管理中心中显示的设备名称。
- d) 在**注册密钥**字段中，输入将机箱配置为由 管理中心管理时所使用的同一注册密钥。

注册密钥是一个一次性的共享密钥。密钥可以包含字母数字字符和连字符（-）。

- e) 在多域部署中，无论当前的域是什么，都将该机箱分配给**叶域**。

如果当前域是叶域，机箱会自动添加到当前域。如果当前域不是叶域，则注册后必须切换到叶域才能配置机箱。一个机箱只能属于一个域。

- f) （可选）将机箱添加到 **设备组**。
- g) 如果在机箱安装过程中使用了 NAT ID，请展开并在 **唯一 NAT ID** 字段中输入相同的 NAT ID。

NAT ID 可以包含字母数字字符和连字符（-）。

- h) 点击 **Submit**。

机箱将添加到 **设备 > 设备管理** 页面。

向新的管理中心注册

此程序显示如何使用新的 管理中心 进行注册。即使新的 管理中心 使用旧的 管理中心 的 IP 地址，也应执行这些步骤。

过程

步骤 1 在旧 管理中心 上，如果存在，请取消注册托管设备。请参阅[从管理中心取消注册设备](#)，第 54 页。

如果您有与 管理中心的活动连接，则无法更改 管理中心 IP 地址。

步骤 2 连接到设备 CLI，例如使用 SSH。

步骤 3 配置新的 管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE } regkey [nat_id] [display_name]
```

- {hostname | IPv4_address | IPv6_address}-设置主机名，IPv4地址或IPv6地址。管理中心
- **DONTRESOLVE**-如果 管理中心 不可直接寻址，请使用 **DONTRESOLVE** 而不是主机名或 IP 地址。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。当您将此设备添加到 管理中心时，请确保同时指定设备 IP 地址和 *nat_id*；连接的一端需要指定 IP 地址，两端需要指定相同的唯一 NAT ID。
- *regkey*-输入注册期间要在 管理中心 和设备之间共享的注册密钥。可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加威胁防御时，需要在管理中心上输入相同的密钥。

- **nat_id**-当一方未指定 IP 地址时，在管理中心与设备之间的注册流程中使用的字母数字字符串，介于 1 至 37 个字符。此 NAT ID 是仅在注册期间使用的一次性密码。确保 NAT ID 是唯一的，不会被等待注册的任何其他设备使用。添加威胁防御时，在管理中心上指定相同的 NAT ID。
- **display_name** - 使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 CDO 标识为仅用于分析的主用管理器和本地部署管理中心，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称：
 - **hostname | IP_address**（如果不使用 **DONTRESOLVE** 关键字）
 - **manager-timestamp**

示例：

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

步骤 4 将此设备添加到管理中心。

解决序列号（零接触调配）注册问题

如果设备无法使用序列号进行注册，则设备可能未成功连接到云。要确认云连接，请检查托管状态 LED 是否呈绿色闪烁。如果它没有呈绿色闪烁，则可能是由于以下原因导致的：

- 您在 CLI 或 设备管理器 中执行了初始配置，并禁用了低接触调配
- 序列号已被其他管理器申领

有关序列号注册的其他要求，请参阅[使用序列号添加设备（零接触调配）](#)，第 38 页。

要解决注册失败问题，请执行以下任务之一。

重置设备

在以下型号上支持：

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100

如果您无权访问 CLI，并希望确保您的设备已取消配置并为 零接触调配做好准备，请按住凹进的小重置按钮五秒钟以上，将设备重置为默认状态。有关详细信息，请参阅硬件安装指南。

使用手动注册和注册密钥

如果低接触调配失败，完成注册的最简单方法是使用注册密钥方法。

1. 请参阅[为手动注册完成威胁防御初始配置](#)，第 12 页或[使用设备管理器完成威胁防御初始配置](#)，第 12 页。
2. 如果系统未显示初始设置任务，则可能是您的设备已成功注册到另一个管理中心。您必须先删除管理连接，然后再向正确的管理器重新注册。
 1. 首先，检查注册是否已完成：

```
> 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
```

2. 如果注册 (Registration) 显示已完成 (Completed)，则需要删除管理器：
configure manager delete
3. 然后，您可以使用 **configure manager add** 在 CLI 上注册设备。

在 CLI 中重新启动低接触调配

如果设备之前使用低接触调配进行了注册，则注册将失败，您将在 CDO 中看到序列号已申领 (Serial Number Already Claimed) 错误。

您可以取消注册序列号，清除配置和任何现有管理连接，然后重新开始该过程。

1. 使用 SSH 或控制台端口连接到 FXOS CLI。

如果使用 SSH，则连接到 威胁防御 CLI。在这种情况下，请输入 **connect fxos**。如果使用控制台端口，则直接连接到 FXOS。

```
> connect fxos
firepower#
```

2. 进入本地管理模式。

connect local-mgmt

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

3. 从思科云取消注册设备。

cloud deregister

```
firepower(local-mgmt)# cloud deregister
Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
```

```
2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

- 清除配置以恢复云连接。

erase configuration

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

- 使用序列号添加设备（零接触调配），第 38 页

使用设备管理器重新启动低接触调配

如果您登录设备管理器，可能会意外禁用低接触调配。在这种情况下，您可以在设备管理器中重新启动低接触调配。



注释 如果序列号已被申领，请参阅在 [CLI 中重新启动低接触调配](#)，第 53 页。

- 在设备管理器中，点击设备 (Device)，然后点击系统设置 (System Settings) > 云服务 (Cloud Services)。
- 选中自动注册 思科防御协调器 或 Cisco Secure Firewall Management Center。
- 点击注册 (Register)。
- 使用序列号添加设备（零接触调配），第 38 页

从管理中心取消注册设备

如果不希望再管理设备，可以将其从管理中心中取消注册。

要取消注册集群、集群节点或高可用性对，请参阅这些部署的章节。

取消注册设备：

- 会切断管理中心和该设备之间的所有通信。
- 从设备管理 (Device Management) 页面删除设备。
- 如果设备的平台设置策略配置为使用 NTP 从管理中心接收时间，则将设备返回本地时间管理。
- 保持配置不变，以便设备继续处理流量。

NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将设备再次注册到相同或不同的管理中心会导致配置被删除，因此设备将在该点停止处理流量。

在取消注册设备之前，请务必导出配置或创建模板，以便在重新注册设备时可以重新应用设备级配置（接口、路由等）。如果您没有已保存的配置或模板，则必须重新配置设备设置。

重新添加设备并导入已保存的配置、使用模板或重新配置设置后，您需要先部署配置，然后才能再次开始传递流量。

开始之前

要重新应用设备级配置（如果您将其重新添加到管理中心），请执行以下操作之一：

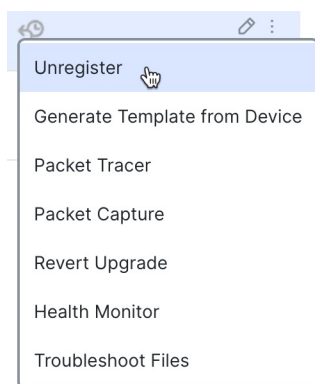
- 导出设备配置。请参阅[导出和导入设备配置](#)。
- 创建用于设备的模板。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要取消注册的设备旁边点击 **更多** (⋮)，然后点击**取消注册 (Unregister)**。

图 27: 取消注册



步骤 3 确认您要取消注册设备。

步骤 4 您现在可以更改管理器。

- 向此管理中心重新注册设备 - 如果您知道注册密钥和 NAT ID，则可以[使用注册密钥添加设备](#)，第 29 页。如果您需要重置它们，则可以像新配置一样重新配置管理器。请参阅[向新的管理中心注册](#)，第 51 页。
- 注册到新的管理中心 - [向新的管理中心注册](#)，第 51 页。
- 更改为设备管理器 - [从管理中心切换到设备管理器](#)，第 66 页。
- 删除管理器而不指定新管理器 - 要在不识别新管理器的情况下切断威胁防御上的管理连接（无管理器模式），请在威胁防御 CLI 中使用 **configure manager delete** 命令。

关闭或重新启动设备

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

请参阅以下任务以正确关闭或重启系统。



注释 重新启动设备后，您可能会看到无法重新建立管理连接的错误。在某些情况下，在设备上的管理接口准备就绪之前尝试连接。系统将自动重试连接，并应在 15 分钟内建立连接。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要重新启动的设备旁边，点击 **编辑** (✎)。

步骤 3 点击设备 (Device)。

步骤 4 要重启设备：

- 请点击 **重启设备** (↺)。
- 出现提示时，确认是否要重启设备。

步骤 5 要关闭设备：

- 在**系统 (System)** 部分中点击 **关闭设备** (⏻)。
- 出现提示时，确认是否要关闭设备。
- 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

对于 ISA 3000，完成关闭后，系统 LED 将熄灭。至少等待 10 秒，然后再断开电源。

下载托管设备列表

您可以下载所有托管设备的报告。

开始之前

要执行以下任务，您必须是管理员用户。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 点击 [下载设备列表报告](#) 链接。

步骤 3 您可以下载 CSV 或 PDF 格式的设备列表。选择 [下载 CSV](#) 或 [下载 PDF](#) 以下载报告。

将配置迁移到新型号

Cisco Secure Firewall Threat Defense 模型迁移向导使您能够将配置从旧模型迁移到新模型。您可以将源设备接口映射到目标设备接口。在迁移之前，源设备和目标设备已锁定。

支持进行迁移的设备

支持的源设备

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140



注释 源设备必须为 7.0 或更高版本。

支持的目标设备

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140



注释 Cisco Secure Firewall 3110、3120、3130 和 3140 设备必须为 7.1 或更高版本。Cisco Secure Firewall 3105 必须为 7.3 或更高版本。

迁移许可证

您必须使用智能许可帐户注册和注册设备。迁移会将源设备许可证复制到目标设备。

迁移的前提条件

- 您必须将源设备和目标设备注册到管理中心。
- 您的智能许可帐户必须具有目标设备的许可证授权。
- 我们建议目标设备是没有任何配置的新注册设备。
- 源设备和目标设备必须处于同一：
 - 域
 - 防火墙模式：路由或透明
 - 合规模式
- 目标设备不得：
 - 在多实例模式下
 - 是集群的一部分
- 用户必须在设备上具有修改权限。
- 源设备上的配置必须有效且没有错误。
- 源设备可以有待处理的部署。但在迁移期间，不得在任何设备上运行部署、导入或导出任务。
- 如果源设备是 HA 对的一部分，目标设备不需要是 HA 对的一部分，反之亦然。迁移不会形成或破坏 HA 对。

向导可以迁移哪些配置？

迁移向导会将以下配置从源设备复制到目标设备：

- 许可证
- 接口配置
- 内联集配置
- 路由配置
- DHCP 和 DDNS 配置

- 虚拟路由器配置
- Policies
- 关联的对象和对象覆盖
- 平台设置
- 远程分支机构部署配置

迁移向导会将以下策略配置从源设备复制到目标设备：

- 运行状况策略
- NAT 策略
- QoS 策略
- 远程访问 VPN 策略
- FlexConfig 策略
- 访问控制策略
- 预过滤策略
- IPS 策略
- DNS 策略
- SSL 策略
- 恶意软件和文件策略
- 身份策略

迁移向导会将以下路由配置从源设备复制到目标设备：

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- 基于策略的路由
- Static Route
- 组播路由
- 虚拟路由器

迁移向导会将以下接口从源设备复制到目标设备：

- 物理接口
- 子接口
- Etherchannel 接口
- 网桥组接口
- VTI 接口
- VNI 接口
- 环回接口

迁移的限制

- 向导不会迁移：
 - 站点间 VPN
 - SNMP 配置

在迁移后，您可以使用设备的平台设置来配置 SNMP。
- 一次只能执行一个迁移。
- 如果源接口的速度、自动协商和双工设置对于目标设备的映射接口有效，则会复制这些值。否则，这些参数将被设置为默认值。
- 远程访问 VPN 信任点证书不会被注册。您必须在部署之前手动注册这些证书。
- 在迁移后，默认情况下，目标设备会使用 Snort 3 而不是 Snort 2，即使源设备使用的是 Snort 2。
- 对于 HA 设备：
 - 目标设备：您不能映射属于故障转移配置的接口。这些接口会在向导中被禁用。
 - 源和目标设备：被监控的接口、故障转移触发条件和接口 MAC 地址等 HA 配置不会被向导迁移。如果需要，您必须在迁移后手动配置这些参数。

迁移 Cisco Secure Firewall Threat Defense

开始之前

查看迁移的前提条件和限制。

过程

步骤 1 选择设备 > 设备管理。

- 步骤 2** 点击页面右上角的**迁移 (Migrate)**。
- 步骤 3** 点击欢迎屏幕上的**开始 (Start)**。
- 步骤 4** 从**源设备 (Source Device)** 下拉列表中选择设备。
- 如果设备是 HA 对的一部分，则仅显示 HA 对的容器名称。
- 步骤 5** 点击**下一步 (Next)**。
- 步骤 6** 从**源设备 (Source Device)** 下拉列表中选择设备。
- 如果设备是 HA 对的一部分，则仅显示 HA 对的容器名称。
- 步骤 7** 点击**下一步 (Next)**。
- 步骤 8** 在**配置接口 (Configure Interfaces)** 步骤中，将源设备的物理接口映射到目标设备的物理接口。
- 并非强制映射所有接口。您必须映射所有已命名的接口和属于其他接口的接口。您不能映射属于 HA 故障转移配置的接口。这些接口会在向导中被禁用。向导会根据用户提供的接口映射来创建逻辑接口。
- 点击**映射默认值 (Map Default)** 以配置默认的接口映射。
- 例如，源设备中的以太网接口 1/1 会被映射到目标设备中的以太网接口 1/1。
- 点击**全部清除 (Clear All)** 可清除所有映射。
- 步骤 9** 点击**下一步 (Next)**。
- 步骤 10** 点击**查看映射 (View Mappings)** 以验证接口映射。
- 步骤 11** 点击**提交 (Submit)** 开始迁移。
- 步骤 12** 在**通知 (Notifications) > 任务 (Tasks)** 页面中查看迁移状态。

下一步做什么

在成功迁移后，您可以部署设备。

部署并非强制性的，您可以验证配置并根据需要进行部署。但是，在部署之前，请确保执行 [迁移最佳实践](#)，第 61 页中提到的操作。

迁移最佳实践

成功迁移后，我们建议您在部署之前执行以下操作：

- 如果源设备处于活动状态，请更改接口的 IP 地址，因为它们会从源设备复制到目标设备。
- 确保使用修改后的 IP 地址来更新 NAT 策略。
- 如果在迁移后将接口速度设置为默认值，请配置接口速度。
- 在目标设备上重新注册设备证书（如有）。
- 如果您有 HA 设置，请配置 HA 参数，例如被监控的接口、故障转移触发条件和接口 MAC 地址。

- 配置迁移后重置的诊断接口。
- （可选）使用设备的平台设置来配置 SNMP。
- （可选）配置远程分支机构部署配置。

如果源或目标设备具有通过数据接口的管理器访问权限，则在迁移后，管理器访问权限将丢失。更新目标设备上的管理器访问配置。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南 或联机帮助中的将管理器访问接口从“管理”更改为“数据”主题。

- （可选）根据需要配置站点间 VPN。这些配置不会从源设备迁移。
- 在部署之前查看部署预览。选择 **部署 > 高级部署**，然后点击设备的 **预览** (📄) 图标。

交换机管理器

如果需要，您可以切换管理器。

从设备管理器切换到管理中心

当您从设备管理器切换到管理中心时，除管理接口和管理器访问设置外，所有接口配置会被保留。请注意，不会保留其他配置设置，例如访问控制策略或安全区。

切换到管理中心后，您将无法再使用设备管理器管理威胁防御设备。

开始之前

如果防火墙已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 在设备管理器中，从思科智能软件管理器中取消注册设备。

步骤 2 （可能需要）配置管理接口。

您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用设备管理器连接的管理接口，则必须重新连接到设备管理器。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。
- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

步骤 3 选择 设备 (Device) > 系统设置 (System Settings) > 集中管理 (Central Management)，然后点击继续 (Proceed) 以设置 管理中心 管理。

步骤 4 配置管理中心/CDO 详细信息。

图 28: 管理中心/CDO 详细信息

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

☒ Yes ☐ No

Threat Defense
10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO
10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

••••• 

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

☐ Data Interface

Please select an interface ▼

☒ Management Interface [View details](#)

CANCEL CONNECT

- a) 对于是否知道管理中心/CDO 主机名或 IP 地址？，如果您可以使用 IP 地址或主机名访问管理中心，请点击是，如果管理中心CDO 位于 NAT 之后或没有公共 IP 地址或主机名，请点击否。

必须至少有一个设备（管理中心或威胁防御设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。

- b) 如果您选择是 (Yes)，则输入管理中心/CDO 主机名或 IP 地址。
c) 指定管理中心/CDO 注册密钥。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 可用于将多台设备注册到管理中心。

- a) 指定 NAT ID。

此 ID 是您选择的唯一一次性字符串，您还需要在管理中心上指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。我们建议您始终使用 NAT ID，即使它是可选的，但在以下情况下必须使用：

- 您将管理中心 IP 地址设置为 DONTRESOLVE。
- 在管理中心上添加设备时，您没有指定可访问的设备 IP 地址或主机名。
- 即使双方都指定了 IP 地址，也只能使用数据接口进行管理。
- 管理中心使用多个管理接口。

步骤 5 配置连接配置。

- a) 指定 FTD 主机名。

如果您使用数据接口进行管理中心/CDO 访问接口访问，则此 FQDN 将用于此接口。

- b) 指定 DNS 服务器组。

选择现有组或创建一个新组。默认 DNS 组名为 CiscoUmbrellaDNSServerGroup，其中包括 OpenDNS 服务器。

如果要为管理中心/CDO 访问接口选择数据接口，则此设置会设置数据接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您将威胁防御设备添加到管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御设备同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。

如果要为管理中心/**CDO 访问接口**/**FMC 访问接口**选择管理接口，则此设置会配置管理 DNS 服务器。

- c) 对于**管理中心/CDO 访问接口**，请选择任何已配置的接口。

将威胁防御设备注册到管理中心后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 6（可选）如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到管理中心之前手动配置默认路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。

步骤 7（可选）如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保管理中心可接通完全限定域名 (FQDN) 的威胁防御设备。参阅**设备 > 系统设置 > DDNS 服务**配置动态 DNS。

如果您在将威胁防御设备添加到管理中心之前配置 DDNS，则威胁防御设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (<https://help.dyn.com/remote-access-api/>)。

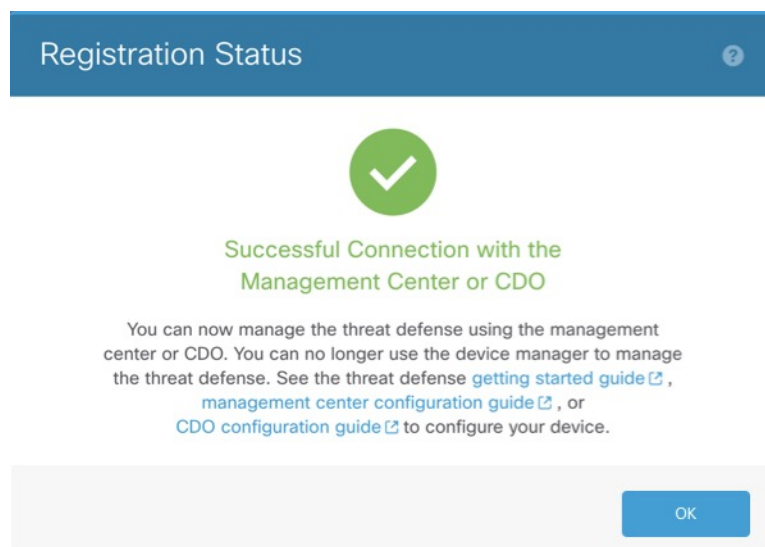
使用管理接口访问管理器时，不支持 DDNS。

步骤 8 点击**连接 (Connect)**。**注册状态**对话框显示切换到管理中心的当前状态。在**保存管理中心/CDO 注册设置**步骤后，转到管理中心，并添加防火墙。

如果要取消切换到管理中心，请点击**取消注册**。否则，请在**保存管理中心/CDO 注册设置**步骤之后关闭设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果您在**保存管理中心/CDO 注册设置**步骤后保持连接到设备管理器，您最终将看到与**管理中心/CDO**成功连接对话框。您将断开与设备管理器的连接。

图 29: 成功连接



从管理中心 切换到 设备管理器

您可以将当前由本地部署或云交付的管理中心管理的威胁防御设备配置为使用设备管理器设备。

您可以从管理中心切换到设备管理器，而无需重新安装软件。在从管理中心切换到设备管理器之前，请确认设备管理器 满足您的所有配置要求。如果要从 设备管理器 切换到 管理中心，请参阅[从设备管理器切换到 管理中心](#)，第 62 页。



注意 切换到 设备管理器 会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

过程

步骤 1 在 管理中心 中，从 **设备 (Devices) > 设备管理 (Device Management)** 页面取消注册防火墙。

步骤 2 使用 SSH 或控制台端口连接到 威胁防御 CLI。如果使用 SSH，请打开与 **管理 IP 地址** 的连接，并使用 **admin** 用户名（或具有管理员权限的任何其他用户）登录 威胁防御 CLI。

控制台端口默认为 FXOS CLI。使用 **connect ftd** 命令连接到 威胁防御 CLI。SSH 会话直接连接到 威胁防御 CLI。

如果无法连接到管理 IP 地址，请执行以下操作之一：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。使用 **configure network ipv4/ipv6 manual** 命令。

步骤 3 验证您当前处于远程管理模式之下。

show managers

示例:

```
> show managers
Type                : Manager
Host                : 10.89.5.35
Display name        : 10.89.5.35
Identifier           : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration         : Completed
```

步骤 4 删除远程管理器，进入无管理器模式。

configure manager delete uuid

无法直接从远程管理转至本地管理。如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

示例:

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

步骤 5 配置本地管理器。

configure manager local

现在，您可以使用 Web 浏览器在 **https://management-IP-address** 位置打开本地管理器。

示例:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Cisco Secure Firewall 3100/4200 上的热插拔 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：威胁防御

- 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。



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 3100
- Cisco Secure Firewall 4200

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 威胁防御 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
```

设备管理的历史记录

功能	管理中心 最低版本	威胁防御 最低版本	详细信息
支持从本地管理中心注册序列号 (零接触调配)。	7.6.0	管理中心必须可公开访问： 7.2.0 已删除限制： 7.2.4/7.4.0	现在，您可以在本地管理中心内使用设备的序列号注册设备。使用模板（需要设备上的威胁防御 7.4.1+），您可以一次注册多个设备。此功能以前称为低接触调配。 需要 思科安全云。对于升级后的管理中心，现有的 CDO 集成将继续有效，直到您启用 思科安全云为止。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 添加 (Add) > 设备（向导）(Device [Wizard]) 支持的平台：Firepower 1000/2100、Cisco Secure Firewall 1200/3100。请注意 Firepower 2100 仅支持威胁防御 7.4.1 - 7.4.x；这些设备无法运行版本 7.6.0。
删除 (Delete) 菜单项被重命名为取消注册 (Unregister)	7.6.0	任意	删除 (Delete) 菜单选项已重命名为取消注册 (Unregister)，以便更好地指示正在从管理中心取消注册设备、高可用性对或集群，而不是从高可用性对或集群中删除或清除其配置。设备、高可用性对或集群继续传递流量，直到重新注册为止。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 更多 (⋮)
使用模板添加设备	7.6.0	7.4	设备 (Devices) > 设备管理 (Device Management) > 添加设备（向导）(Add > Device [Wizard]) 屏幕让您可使用模板来添加设备。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 添加 (Add) > 设备（向导）(Device [Wizard])
禁用 Firepower 1000 和 Cisco Secure Firewall 3100/4200 上的前面板 USB-A 端口。	7.6.0	7.6.0	现在可以禁用 Firepower 1000 和 Cisco Secure Firewall 3100/4200 上的前面板 USB-A 端口。默认情况下，端口处于启用状态。 新增/修改的威胁防御 CLI 命令：system support usb show、system support usb port disable、system support usb port enable 多实例模式下 Cisco Secure Firewall 3100/4200 的新增/修改的 FXOS CLI 命令：show usb-port、disable USB port、enable usb-port 请参阅：Cisco Secure Firewall Threat Defense 命令参考 和 Cisco Firepower 4100/9300 FXOS 命令参考

功能	管理中心 最低版本	威胁防御 最低版本	详细信息
Firepower 4100/9300 的机箱级运行状况警报。	7.4.1	7.4.1	现在，只要将机箱作为只读设备注册到管理中心，您就可以查看 Firepower 4100/9300 的机箱级运行状况警报。您还必须启用防火墙威胁防御平台故障运行状况模块并应用运行状况策略。警报会出现在信息中心、运行状况监控器（在左窗格的“设备” (Devices) 下选择机箱）和运行状况事件视图中。 您还可以在多实例模式下为 Cisco Secure Firewall 3100 添加机箱（并查看运行状况警报）。对于这些设备，您可以使用管理中心来管理机箱。但对于 Firepower 4100/9300 机箱，您仍必须使用机箱管理器或 FXOS CLI。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 添加 (Add) > 机箱 (Chassis)
使用序列号将设备注册 Firepower 1000/2100 和 Cisco Secure Firewall 3100 到管理中心的零接触调配。	7.4.0	管理中心可公开访问：7.2.0 管理中心不可公开访问：7.2.4/7.4.0	通过零接触调配（也称为低接触调配），您可以按序列号将 Firepower 1000/2100 和 Cisco Secure Firewall 3100 设备注册到管理中心，而无需在设备上执行任何初始设置。管理中心与 SecureX 和 CDO 集成以实现此功能。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 添加 (Add) > 设备 (Device) > 序列号 (Serial Number) 版本限制：当管理中心无法公开访问时，7.3.x 或 7.4.0 版威胁防御设备不支持此功能。支持在版本 7.4.1 中返回。

功能	管理中心 最低版本	威胁防御 最低版本	详细信息
合并的管理接口和诊断接口。	7.4.0	7.4.0	升级影响。升级后合并接口。 对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。 如果您已升级到 7.4 或更高版本，并且： • 您没有为诊断接口进行任何配置，则接口将自动合并。 • 您已为诊断接口进行了配置，则可以选择手动合并接口，也可以选择继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。 合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。 对于平台设置，这意味着： • 您无法再启用 HTTP、ICMP 或 SMTP 进行诊断。 • 对于 SNMP，可以允许“管理”而不是“诊断”上的主机。 • 对于系统日志服务器，您可以通过“管理”而不是“诊断”来访问它们。 • 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。 • 如果不指定接口，DNS 查找不会再回退到管理专用路由表。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 接口 (Interfaces) 新增/经修改的命令：show management-interface convergence
从 Firepower 1000/2100 迁移到 Cisco Secure Firewall 3100。	7.4.0	任意	您现在可以将配置从 Firepower 1000/2100 轻松迁移到 Cisco Secure Firewall 3100。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 迁移 (Migrate) 平台限制：不支持从 Firepower 1010 或 1010E 迁移。
下载所有已注册设备的报告。	7.4.0	任意	现在您可以下载所有已注册设备的报告。在设备 (Devices) > 设备管理 (Device Management)中，点击页面右上角新的下载设备列表报告 (Download Device List Report)链接。

功能	管理中心 最低版本	威胁防御 最低版本	详细信息
使用数据接口管理威胁防御高可用性对。	7.4.0	7.4.0	威胁防御高可用性现在支持使用常规数据接口与管理中心通信。以前，只有独立设备才支持这一功能。 请参阅： 使用威胁防御数据接口进行管理
ISA 3000 系统 LED 支持关闭。	7.0.5/7.3.0	7.0.5/7.3.0	关闭 ISA 3000 时，系统 LED 会熄灭。至少等待 10 秒，然后再断开电源。
ISA 3000 支持关闭。	7.0.2/7.2.0	7.0.2/7.2.0	您现在可以关闭 ISA 3000；以前，您只能重新启动设备。
多管理器支持	7.2.0	7.2.0	我们引入了云交付的管理中心。云交付的管理中心使用 思科防御协调器 (CDO) 平台，并会跨多个思科安全解决方案统一管理。我们负责管理器的更新。 运行版本 7.2+ 的硬件或虚拟管理中心可以“共同管理”云托管设备，但仅限于事件日志记录和分析目的。您无法从硬件或虚拟管理中心将策略部署到这些设备。 新增/修改的命令： configure manager add, configure manager delete, configure manager edit, show managers 新增/修改的屏幕： - 将云托管设备添加到硬件或虚拟管理中心时，请使用新的CDO 托管设备复选框将其指定为仅用于分析。 - 在 设备 > 设备管理 中查看哪些设备仅用于分析。 有关详细信息，请参阅 CDO 文档。
Cisco Secure Firewall 3100 上的 SSD 支持 RAID。	7.1.0	7.1.0	SSD 是自加密驱动器 (SED)，如果您有 2 个 SSD，则它们会组成软件 RAID。 新增/经修改的命令： configure raid, show raid, show ssd
管理连接支持 TLS 1.3。	7.1.0	7.1.0	FMC 设备管理连接现在使用 TLS 1.3。以前支持 TLS 1.2。
使用 FDM 将 FTD 配置为由 FMC 进行管理。	7.1.0	7.1.0	如果使用 FDM 执行初始设置，那么在切换到 FMC 进行管理时，除管理和 FMC 访问设置外，会保留在 FDM 中完成的所有接口配置。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 FMC CLI 时，仅保留管理和管理器访问设置（例如，不保留默认的内部接口配置）。 切换到 FMC 后，您将无法再使用 FDM 管理 FTD。 新增/修改 FDM 屏幕： 系统设置 (System Settings) > 管理中心 (Management Center)

功能	管理中心 最低版本	威胁防御 最低版本	详细信息
按升级状态过滤设备。	6.7.0	6.7.0	设备管理 (Device Management) 页面现在提供有关托管设备的升级信息，包括设备是否正在升级（及其升级路径），以及上次升级是成功还是失败。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management)
一键访问 Firepower 机箱管理器。	6.4.0	6.4.0	对于 Firepower 4100/9300 系列设备，“设备管理” (Device Management) 页面会提供指向 Firepower 机箱管理器 Web 界面的链接。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management)
按运行状况和部署状态过滤设备；查看版本信息。	6.2.3	6.2.3	“设备管理” (Device Management) 页面现在提供托管设备的版本信息，并且能够按运行状况和部署状态过滤设备。 新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management)

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。