使用设备模板进行设备管理

您可以使用设备模板将设备添加到 防火墙管理中心。

关于使用设备模板进行设备管理

通过设备模板，可以部署具有预配置初始设备配置的多个分支设备。您可以使用设备模板对多台设备执行批量零接触调配，对具有不同接口配置的多台设备应用day 2配置更改，以及从现有设备克隆配置参数。 您也可以使用序列号一次向 防火墙管理中心 注册多个设备。

使用基本初始配置注册设备时，可以应用访问控制策略和许可证等有限配置。然后，您必须在设备注册后单独配置其他设备设置，如接口、路由和站点间VPN配置。设备模板可让您预先配置这些设置及其他设置，以便在注册时应用。每个设备需要唯一的值，如IP地址，可以使用在注册时定义的变量和网络对象覆盖来定义。

您还可以在设备模板中配置站点间VPN连接。这些配置定义了设备应加入的站点间VPN拓扑。VPN配置以及其他设备模板策略和配置可使分支设备轻松部署到网络中。设备模板仅支持将设备配置为分支设备。一台设备可以是多个中心辐射型站点间 VPN 拓扑的一部分。

将配置的设备模板应用于设备后，解析变量，配置受保护的网络覆盖，然后将该设备添加为指定 VPN 拓扑中的分支。

使用模板注册设备的方法

您可以通过以下方法，使用设备模板在 防火墙管理中心 上注册设备并设置 Day 0 配置：

- 注册密钥 - 您可以通过在 防火墙管理中心 中指定注册密钥并定义变量来注册单个设备。
- 序列号 - 您可以使用零接触调配按序列号注册一个或多个设备。对于序列号注册，请在您上传的 CSV 文件中定义所有变量和覆盖。

变量和网络对象覆盖

您可以使用变量和网络对象覆盖对模板配置进行参数化。

变量是模板配置支持的对象类型。模板中的变量定义设备的特定配置值。您可以在设备注册和在设备上应用模板时定义这些变量的值。您可以在使用变量的字段看到变量图标 (x)。变量显示时使用 $ 前缀，以区别这些值和其他值。

有关支持的变量类型和创建变量的信息，请参阅支持的变量和添加变量。

网络对象覆盖类似于变量。但是，这些值用于为网络对象提供覆盖值。您可以在模板中声明网络对象列表，并为这些对象创建网络对象覆盖。然后，您就可以在设备上应用模板时为这些网络对象覆盖提供值。例如，如果在模板中定义了主机网络对象，则可以在设备上应用模板之前添加网络对象覆盖，然后在设备上应用模板时提供相关值。

有关受支持的网络对象和添加网络对象覆盖的详细信息，请参阅支持的网络对象覆盖和添加网络对象覆盖。

型号映射

由于不同型号设备的接口配置各不相同，因此必须将模板中的接口配置复制到设备上的目标接口。通过模型映射，可以定义模板中定义的接口与所需 模型接口的映射。在设备上应用模板时，接口配置中的变量会被替换为您提供的值，并复制到设备上的映射接口。请注意，在设备上开始应用模板之前，必须在模板中创建模型映射。有关设置模型映射的详细信息，请参阅添加模型映射。

模板和高可用性

设备注册后，可以在 高可用性设备上应用设备模板。设备模板不支持特定于高可用性的配置。目标高可用性设备对配置中已包含的任何高可用性配置和受监控接口不会被修改。您无法将任何模板接口映射到故障转移接口。

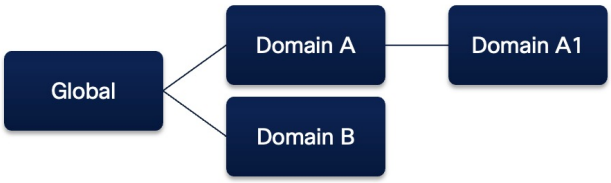
可以从高可用性设备对生成设备模板。模板操作（如在设备上应用模板、生成模板、导入和导出模板）只能在主用设备上执行。不能在备用设备上执行这些操作。

模板和域

设备模板可以存在于任何域中。如果您在子域中，则对域层次结构中您上面的模板具有只读访问权限。您可以将模板应用于其域或其父域中的设备。您可以从设备生成模板，并将该模板应用于域层次结构中任意域的设备。

下面给出了一个域层次结构示例，以及一个显示支持的设备模板应用和生成场景的表格。

请考虑以下情景：



- 域 A 和域 B 是全局域的子域。
- 域 A1 是域 A 的子域。

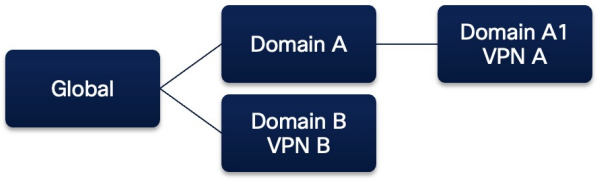
模板域	设备领域	支持的设备模板应用/生成
全局	A1	是
全局	B	是
A	A1	是
A	B	否
B	A1	否
B	B	是
A1	A1	是
A1	B	否

域和 VPN 连接

- 您可以在全局域或子域/枝叶域中定义模板，但只能在枝叶域中定义 VPN 拓扑。
- 您可以在模板中为所有域配置 VPN 连接。在模板应用过程中，只有当设备与 VPN 拓扑处于同一域时，VPN 连接才会应用到设备。

下面给出了一个域层次结构示例，以及一个显示支持的设备模板应用和生成场景的表格。

请考虑以下情景：



- 域 A 和域 B 是全局域的子域。
- 域 A1 是域 A 的子域。
- VPN A 是域 A1 的一部分。
- VPN B 是域 B 的一部分。

模板域	模板中的 **VPN** 拓扑	设备领域	支持的设备模板应用/生成
全局	VPN A VPN B	A1	否
全局	VPN B	B	是
A	VPN A	A1	是
B	VPN B	A1	否
B	VPN B	B	是
A1	VPN A	A1	是

在设备上应用模板前后验证模板配置

在设备上应用模板前后执行模板配置验证。

任务开始时会执行以下验证检查，以便在设备上应用模板：

- 确保支持目标设备型号和版本。
- 集群和容器检查 - 设备不得是集群或多实例的一部分。
- 模型映射验证 - 目标设备型号的模型映射存在且有效。
- 对模板参数值进行合理性检查。例如，用作接口 IP 地址的两个变量的值不能相同。

任务结束时将执行以下验证检查，以便在设备上应用模板，确保应用的配置有效：

- 接口配置验证。例如，两个或多个接口的 IP 地址字段所用变量的 IP 地址值不得相同。
- 路由策略验证。例如，BGP 邻居配置中的 IPv4 地址不得与任何接口的 IP 地址重叠。

如果在设备上应用模板的任务结束时进行的验证检查失败，任何应用的配置都将回滚，设备将恢复到原始状态。

使用设备模板进行设备管理的要求和前提条件

型号支持

本地 防火墙管理中心、云交付的防火墙管理中心 (cdFMC) 以及运行 Cisco Secure Firewall 版本 7.4.1 及更高版本的以下型号支持设备模板：

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 1200
- Firepower 2100（仅限 7.4.x）
- Cisco Secure Firewall 3100

支持的域

任意

用户角色

- 要创建、修改或删除模板，请执行以下操作：
  - 管理
  - 网络管理员
- 要查看已创建的模板，请执行以下操作：
  - 任意

设备模板中 VPN 连接的前提条件

- 配置设备模板中必须使用的站点间 VPN 拓扑。
- 确保已配置所有与中心和 VPN 拓扑相关的配置，例如身份验证方法、IKE 和 IPsec 策略。
- 支持的 VPN 中心辐射型拓扑类型包括：
  - 基于策略
  - 基于路由
  - SD-WAN

- 为设备的接口分配适当的逻辑名称和 IP 地址。例如，使用 内部 表示连接到 LAN 的接口，使用 外部 表示连接到互联网或 WAN 的接口。
- 分支设备的版本必须为 7.4.1 及更高版本。

使用设备模板进行设备管理的许可证

- 设备模板没有任何特定的许可证要求。
- 智能许可账户中必须有目标设备的许可权限。
- 要在模板中配置 VPN 连接，Essential 许可证必须允许出口控制功能。选择 **系统** (⚙) > **许可证** > **智能许可证** 在 防火墙管理中心 中验证此功能。
- 在设备上应用模板时，请注意以下有关安全客户端许可的条件：

具有安全客户端许可证的设备	具有安全客户端许可证的模板	设备模板应用后的安全客户端许可证
是	是	模板许可证
是	否	设备许可证
否	是	模板许可证

使用设备模板的设备管理的准则和限制

设备模板的一般准则

- 支持 VNI 和 VTEP 以外的所有设备配置。
- 您可以将共享策略和 S2S VPN 策略附加到模板。这些策略是在模板应用期间分配的。
- 模板可在 HA 设备上应用。但是，不支持在 HA 设备对注册期间应用设备模板。您也无法管理与 HA 相关的配置，例如故障切换链路、备用 IP 地址等。有关详细信息，请参阅威胁防御 HA 设备上的设备模板操作。
- 仅在活动 防火墙管理中心 中支持设备模板操作。备用对等体不支持设备模板操作。
- 确保模板名称和设备显示名称不相同。
- 确保在设备备份或还原操作期间不创建或删除模板。
- 在设备上应用模板后，如果管理器访问从管理接口改为数据接口（反之亦然），则必须重新建立与设备的管理连接。请注意，在模板应用过程中不能更改管理器访问接口。
- 您最多可以将 250 个设备模板添加到 防火墙管理中心。

- 为通过数据接口管理的设备创建和配置的模板不能用于注册和应用到通过管理接口管理的设备。
- 设备注册和模板应用不属于变更管理工作流程。只使用经批准的数据，如访问策略、模板、模板变量、模板中声明的网络覆盖以及模板应用操作中使用的模板配置。
- 每次只支持一台设备使用序列号和访问控制策略进行设备注册。
- 在使用序列号添加设备时，不支持具有 IPv6 DHCP 可发现性的设备。
- 在将模板应用于已注册设备时，模板中的配置只会复制到目标设备。然后，您可以选择在设备上手动部署配置，或者让复制的配置留在设备上，稍后再部署。但是，如果在设备载入过程中应用模板，模板中的配置就会复制到目标设备，并按照现有行为，在设备注册后自动部署到设备上。
- 模型映射中的任何更改都会导致设备被标记为“不同步”(Out of Sync)。如果您对相应模型映射中的接口映射进行了更改，或者在上次应用模板后对配置进行了更改，请考虑将模板重新应用到设备上。
- 设备模板只支持合并的管理和诊断接口。有关详细信息，请参阅合并管理接口和诊断接口。
- 变更管理支持模板配置更新。变更管理不支持创建和应用设备模板。
- 您无法将配置更改从设备同步到模板。下面列出了一些可能需要使用模板更改设备配置的场景以及推荐的解决方案：
  - 如果您想先在一台设备上测试新的配置更改，然后再将更改传播到多台设备上，则建议您在模板中进行更改，并将模板应用到一台设备上。验证该设备上的更改，然后将模板应用到其他设备。
  - 如果要在一台设备上进行大量更改，从而导致与当前配置有明显偏差，然后将这些更改传播到其他设备，则可以选择以下选项之一：
    - 导出当前模板以获取模板副本。然后，您就可以在模板中进行所需的更改，并应用到单个设备。验证该设备上的更改，然后将模板应用到其他设备。
    - 您也可以在设备上进行所需的更改，然后从该设备创建模板。然后，您就可以在其他设备上应用和验证更改。但我们不建议这样做，因为创建的模板中不会出现变量和网络对象覆盖等模板参数。
  - 如果特定设备上的配置与模板中的配置开始出现显着差异，您也可以选择对此设备不使用模板，并从**关联设备 (Associated Devices)** 窗口中删除设备-模板关联。

设备模板中的 VPN 连接准则

- VPN 拓扑支持的接口包括：

拓扑类型	接口类型

基于策略的 SD-WAN	• 物理接口
	  • 非管理
	  • 接口模式必须为“路由”或“无”
	• 子接口
	• 冗余接口
	• Etherchannel 接口
	• VLAN 接口

基于路由	静态虚拟隧道接口

- 在作为VPN拓扑一部分的设备上应用模板时，必须确保模板包含拓扑中使用的所有接口的接口配置。
- 在将具有 VPN 连接的模板应用于多个设备时，请注意以下事项：

  模板会按照您选择设备的顺序应用于多个设备。如果模板有 VPN 连接，则会锁定相应的 VPN 拓扑。
- 对于 SD-WAN 拓扑 VPN 连接：确保接口的 IP 地址子网与 SD-WAN 中心的 IP 地址池子网不存在冲突。
- 域：
  - 您可以在全局域或枝叶域中定义模板。但只能在枝叶域中定义 VPN 拓扑。
  - 您可以在模板中为所有域配置 VPN 连接。在模板应用过程中，只有当设备与 VPN 拓扑处于同一域时，VPN 连接才会应用到设备。

  有关详细信息，请参阅 模板和域，第 3 页。
- 变更管理：在将设备模板应用到设备之前，确保 VPN 拓扑未被变更管理故障单锁定。

设备模板的限制

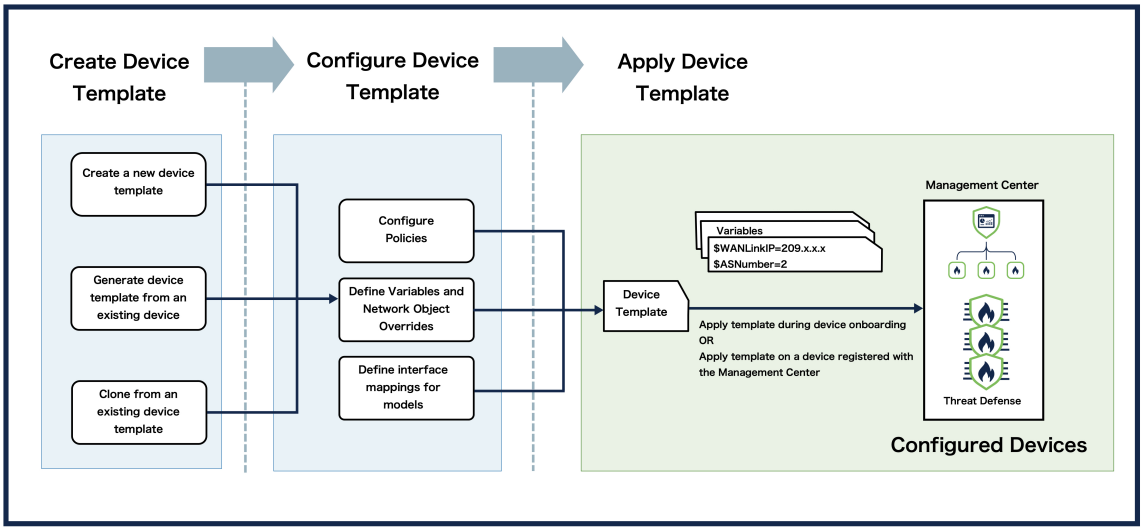
- 使用设备模板不支持以下功能和配置：
  - 多实例模式
  - 集群
  - 非融合管理接口
  - 透明模式
  - HA 故障转移配置

- 机箱配置
- 逻辑设备
- 嵌套对象的变量
- 覆盖对网络组和其他对象类型的支持

VPN 连接的限制

- 当您从属于 VPN 拓扑的设备创建模板时（**设备** > **设备管理** **更多** (⋮) > **从设备生成模板**），VPN 配置不包含在模板中。您必须重新配置模板上的 VPN 配置。
- 当您导出具有一个或多个 VPN 连接的设备模板时（**模板设置 (Template Settings)** > **常规 (General)** > **常规 (General)** 面板 > **导出 (Export)**），不会导出 VPN 连接。您必须在导入的模板上重新配置 VPN 连接。
- 基于证书的身份验证：
  - 设备模板不支持设备的自动证书注册。
  - 在使用带有 VPN 配置的模板载入设备时，如果 VPN 拓扑使用基于证书的身份验证，则设备的首次部署将失败。确保在设备注册后手动注册设备证书，并再次在设备上部署配置。

使用设备模板进行设备管理的工作流程



配置设备模板

添加模板，然后在模板中配置设置。

添加设备模板

您可以添加具有所需配置的新设备模板，或从现有设备生成设备模板。

创建新设备模板

您可以指定设备模板名称、说明、访问控制策略和路由模式。在创建模板后，您可以添加更多配置。执行以下程序来创建设备模板。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击**添加设备模板 (Add Device Template)**。

步骤 3 在**添加设备模板 (Add Device Template)** 窗口中，为模板输入**名称**。

步骤 4 （可选） 输入模板的**描述**。

步骤 5 从下拉列表中选择**访问控制策略 (Access Control Policy)**。

步骤 6 从下拉列表中选择**模式**。

步骤 7 点击**确定**。

从现有设备生成新设备模板

您可以从已在防火墙管理中心注册的设备中生成新的设备模板。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。

执行以下指定的程序，从现有设备生成新设备模板。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **更多** (⋮) 图标，然后点击**从设备生成模板 (Generate Template from Device)**。

步骤 3 在**从设备生成模板 (Generate template from device)** 窗口中，为模板输入**名称**。

步骤 4 （可选） 输入模板的**描述**。

步骤 5 从下拉列表中选择**访问控制策略 (Access Control Policy)**。

注释
此策略将被分配给生成的模板。与生成模板的设备相关联的任何其他共享策略，只有在这些策略在生成模板的域中可见时，才会分配给生成的模板。

步骤 6 点击**确定**。您可以在**通知 (Notifications) > 任务 (Tasks)** 窗口中查看模板创建状态。

步骤 7 选择**设备** > **模板管理**，以查看新创建的模板。

导入设备模板

您可以将模板导入防火墙管理中心或将模板导出到您的本地系统。此功能在以下情况下非常有用：

- 从设备生成模板副本并将其导出，然后将该设备导入另一个 防火墙管理中心 或 云交付的防火墙管理中心。
- 生成模板副本并将其导出，根据需要修改以创建现有模板的变体，然后将模板导入 防火墙管理中心。
- 生成模板的副本并将其导出，然后将该模板导入到源模板在其中不可见的其他域中。

在将模板导入域时，如果导入模板的域中存在同名对象，则配置中的任何对象都会被新建或重复使用。由于域层次结构的原因，任何名称匹配但不可见的对象都会作为新对象导入，名称后缀为 _x。

如果要在使用从其他域克隆的模板的域中导入设备时出现变量名不匹配的情况，则必须在 .csv 文件中指定新的变量名才能导入设备。

执行以下程序，将设备模板从本地系统导入 防火墙管理中心。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要替换为导入模板的模板对应的 **更多** (⋮) 图标。

步骤 3 点击**导入 (Import)**，然后再次点击**导入 (Import)**。

如果要导出模板，点击**导出**，然后点击**确定**。

步骤 4 在**通知 (Notifications) > 任务 (Tasks)** 窗口中查看导入任务的状态。

步骤 5 选择本地系统上的模板 SFO 文件，然后点击**打开 (Open)**。导入的模板 SFO 文件可以新创建、从设备生成或从现有模板克隆。

步骤 6 在**通知 (Notifications) > 任务 (Tasks)** 窗口中查看导入任务的状态。您将看到一条通知，告知您导入或导出任务已成功完成。如果您要导出模板，请在**通知 (Notifications) > 任务 (Tasks)** 窗口中点击**下载导出数据包 (Download Export Package)**，以便将模板配置下载为 SFO 文件。

注释

或者，您也可以转到**模板管理 (Template Management)** 窗口，然后点击模板的 **编辑** (✎) 图标。然后，转至**模板设置 (Template Settings)** > **常规 (General)**，点击**常规 (General)** 磁贴中的**导入 (Import)** 或**导出 (Export)** 以导入或导出模板。

在模板中配置设备设置

创建模板后，您可以设置设备配置，并通过编辑模板配置要在设备上应用的设置。

添加物理接口

默认情况下，设备模板将使设备能够提供以下物理接口：

- 管理接口
- 内部接口
- 外部接口

执行以下程序来创建物理接口。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中添加物理接口的模板的 **编辑** (✎) 图标。

步骤 3 在**接口 (Interfaces)** 选项卡中，点击**添加物理接口 (Add Physical Interface)**。

步骤 4 从下拉列表中选择一个**插槽 (Slot)** 和**端口索引 (Port Index)** 数字。

步骤 5 点击**创建接口 (Create Interface)**。

添加逻辑接口

您可以采用与在防火墙管理中心上相同的方式来创建逻辑接口，而不使用模板。执行以下程序以创建逻辑接口。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中添加逻辑接口的模板的 **编辑** (✎) 图标。

步骤 3 在**接口 (Interfaces)** 选项卡中，点击**添加接口 (Add Interface)**，然后从下拉列表中选择要创建的接口类型。您可以创建以下类型的接口：

- 子接口
- 以太网通道接口
- 桥接组接口
- VLAN 接口
- Virtual Tunnel Interface
- 环回接口

有关详细信息，请参阅接口概述和常规防火墙接口。

编辑接口

您可以采用与在防火墙管理中心上相同的方式来编辑接口，而不使用模板。使用模板变量设置IPv4和 IPv6 地址。设备模板支持 Firepower 1000、Secure Firewall 1200、 Firepower 2100 和 Cisco Secure Firewall 3100 设备上支持的配置。执行以下程序以编辑接口。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中编辑物理接口的模板的 **编辑** (✎) 图标。

步骤 3 在**接口 (Interfaces)** 选项卡中，点击要编辑的接口的**编辑**图标。

步骤 4 在**编辑物理接口 (Edit Physical Interface)** 窗口中，您可以编辑以下任何设置：

- 常规
- PoE
- IPv4
- IPv6
- 路径监控
- 硬件配置
- 管理器访问
- 高级

注释
使用变量配置 IPv4 和 IPv6 地址。有关模板化变量的详细信息，请参阅配置模板参数。

有关编辑上述设置的详细信息，请参阅接口概述和常规防火墙接口。

配置其他设备设置

在不使用模板的情况下，以与 防火墙管理中心 相同的方式配置其他设备设置。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中配置设置的模板的 **编辑** (✎) 图标。

步骤 3 点击窗口顶部的选项卡可配置以下任何设置：

- 内联集
- 路由
- DHCP
- VPN
- 模板设置

配置模板设置

这些是特定于模板的设置，在设备上应用模板时会复制到设备上。在**模板设置 (Template Settings)** 窗口中，您可以配置以下模板设置：

- 常规
  - 常规
  - 许可
  - 应用的策略
  - 高级设置
  - 部署设置
- 模板参数
  - 变量
  - 网络对象覆盖
- 型号映射

编辑常规设置

在**常规 (General)** 磁贴中，您会看到以下字段：

- **模板名称 (Template Name)** – 模板的名称。
- **传输数据包 (Transfer Packets)** - 显示托管设备是否将数据包数据随事件一起发送到管理中心。
- **模式 (Mode)** - 显示设备管理界面的模式：已路由。
- **配置 (Configuration)** - 点击**导出 (Export)** 可将模板配置导出为 SFO 文件。点击**导入 (Import)** 以导入具有所需模板配置的 SFO 文件。
- **按数据接口管理设备 (Manage device by Data Interface)** - 切换按钮以启用或禁用使用数据接口进行设备管理。

执行以下程序编辑设备名称，即可启用或禁用数据包传输。

过程

步骤 1 点击**常规 (General)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 根据您的要求更改**模板名称**。

步骤 3 选中**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。

步骤 4 点击**保存**。

编辑许可证

在**许可证 (License)** 磁贴中，您可以根据模板中使用的配置查看所需的**许可证类型**。在此处选择许可证不会消耗设备上的许可证。只有在将模板应用于设备时才会使用许可证。

执行下面给出的程序，根据您的要求编辑许可证类型。

过程

步骤 1 点击**许可证 (License)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 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 3 点击**保存**。

编辑应用的策略

在**应用的策略 (Applied Policies)** 磁贴中，您可以查看与模板关联的访问控制策略。

对于包含链接的策略，您可以点击链接以查看策略。

执行下面给出的程序，按要求编辑政策任务。

过程

步骤 1 点击**已应用的策略 (Applied Policies)** 磁贴中的 **编辑** (✎) 图标。
步骤 2 对于每种策略类型，请从下拉列表选择一个策略。只有现有的策略会被列出。
步骤 3 点击**保存**。

编辑高级设置

高级设置 (Advanced Settings) 磁贴显示高级配置设置，如下所述。您可以编辑任何这些设置。

表 *1:*“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。
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， 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。 **注释** 默认情况下，在防火墙管理中心中首次添加 时会启用**对象组搜索**。
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。

执行以下程序以编辑高级设置。

过程

步骤 1 点击**高级设置 (Advanced Settings)** 磁贴中的 **编辑** (✎) 图标。

步骤 2 您可以根据需要更改设置。有关详细信息，请参阅以下各节：

- 配置自动应用旁路
- 配置对象组搜索
- 配置接口对象优化

步骤 3 点击**保存**。

编辑部署设置

部署设置 (Deployment Settings) 磁贴显示下表所述信息。

表 2: 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防火墙管理中心访问，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。

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防火墙管理中心访问，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。

执行下面给出的程序以编辑部署设置。

过程

步骤 1 点击**部署设置 (Deployment Settings)** 磁贴中的**编辑 (Edit)** 图标。

步骤 2 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 3 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 (Preview)** 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。
- 在部署历史记录预览中，您可以查看回滚更改。

步骤 4 检查管理连接是否已重新建立。

在 防火墙管理中心中，在 **设备** > **设备管理** > **设备** > **管理** > **FMC 访问详细信息** > **连接状态** 页面上检查管理连接状态。

在 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。

模板模板参数

您可以使用变量和网络对象覆盖等模板参数将配置模板化。

支持的变量

设备模板支持以下变量类型。

变量名称	说明	类型 (Type)
AS 编号	定义唯一的自治系统(AS)编号。	整数 示例：2
FQDN	定义单个完全限定域名(FQDN)。	字符串 示例：abc.example.com
IPv4 主机	定义主机的 IPv4 地址。	字符串 示例：209.165.201.8
IPv4 网络	定义 IPv4 网络地址块。	字符串 示例：209.165.200.224/27
IPv4 范围	定义 IPv4 地址的范围。	字符串 示例： 209.165.200.225-209.165.200.250
IPv6 主机	定义主机的 IPv6 地址。	字符串 示例：2001:DB8::1
IPv6 网络	定义 IPv6 网络地址块。	字符串 示例：2001:DB8:0:CD30::/60
密码	定义密码字符串。	字符串 示例：E28@2OiUrhx!
路由器 ID	定义路由器的标识符。	整数 示例：21

变量名称	说明	类型 (Type)
字符串	定义自定义字符串。	字符串 示例：testvalue2

添加变量

执行以下步骤添加变量。

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**变量 (Variable)**。

步骤 3 点击**添加变量 (Add Variable)**。

步骤 4 输入 **Name**。

在多域部署中，对象名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的对象名称的冲突。

步骤 5 从下拉列表中选择**变量类型 (Variable Type)**：

步骤 6 （可选） 输入**说明**。

步骤 7 点击**保存**。

支持的网络对象覆盖

支持以下网络对象。

网络对象名称	说明	类型 (Type)
网络	地址块，也称为子网。	字符串 示例： IPv4 - 209.165.200.224/27 IPv6 - 2001:DB8::/48
Host	主机的 IP 地址。	字符串 示例： IPv4 - 209.165.200.225 IPv6 - 2001:DB8:1::1

网络对象名称	说明	类型 (Type)
范围	IP 地址范围。	字符串 示例： IPv4 - 209.165.200.225-209.165.200.250 IPv6 - 2001:DB8::1 - 2001:DB8:FFFF:FFFF:FFFF:FFFE:FFFF:FFFF
FQDN	单个完全限定域名 (FQDN)。	字符串 示例：abc.example.com

添加网络对象覆盖

执行下面给出的程序以添加网络对象覆盖。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要在其中添加网络对象覆盖的模板的 **编辑** (✎) 图标。

步骤 3 依次选择**模板设置 (Template Settings)** > **模板参数 (Template Parameters)**。

步骤 4 在**网络对象覆盖 (Network Object Overrides)** 部分中，点击**添加或删除网络对象覆盖 (Add or Remove Network Object Overrides)**。

步骤 5 在**添加或删除网络对象覆盖 (Add or Remove Network Object Overrides)** 窗口中，从**可用网络 (Available Networks)** 窗口中选择要为其创建网络对象覆盖的网络对象，然后点击 > 按钮。

步骤 6 点击**保存**。

添加模型映射

对于每个模型，您可以指定哪个模板接口与哪个模型接口对应。只要接口配置对所有映射型号都有效，就可以将模板映射到一个或多个型号。例如，如果模板包含交换机端口和 VLAN 接口，则该模板只能应用于 Firepower 1010 或 Cisco Secure Firewall 1210/1220。

执行下面给出的程序来添加型号映射。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 对于要在其中创建模型映射的模板，点击**添加模型映射 (Add Model Mapping)**。或者，您可以点击模板的 **编辑** (✎) 图标，然后依次选择**模板设置 (Template Settings)** > **模型映射 (Model Mapping)**。

步骤 3 点击**添加模型映射 (Add Model Mapping)**。

步骤 4 从下拉列表中选择**设备模型 (Device Model)**。

步骤 5 从**模型接口 (Model Interface)** 下拉列表中选择接口，将模板接口映射到设备模型接口。

注释
您可以点击**清除映射 (Clear Mapping)** 以删除已定义的模型映射。点击**重置映射 (Reset Mappings)** 进行默认接口映射，其中映射是根据接口名称的插槽和端口索引顺序进行的。

步骤 6 点击**保存**。接口映射会与设备模型和映射状态一起在**模型映射 (Model Mapping)** 窗口中列出。

注释
可能并非所有设备型号都支持模板中的某些配置。不受支持的配置（如有）不会应用于设备。设备模板应用报告会提供有关此类配置的详细信息。

无效模型映射

可能并非所有设备型号都支持模板中的某些配置。不受支持的配置（如有）不会应用于设备。修改模板配置时，有效的模型映射也可能会失效。例如，在模板上添加新接口并为其分配名称时，必须将新接口映射到设备模型上的相应接口。

以下任意原因都可能让模型映射失效：

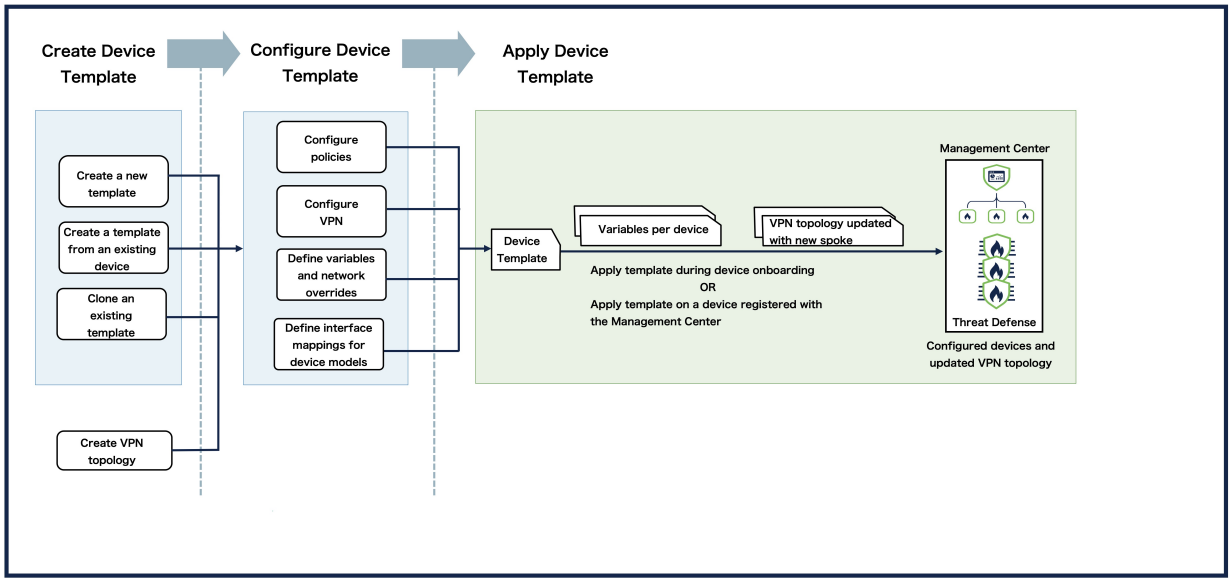
- 配置的 VRF 实例数量超过特定型号的限制。
- 接口映射到不兼容的型号、版本或接口。有关详细信息，请参阅要求和前提条件。
- 接口数量超过型号限制。
- 删除了映射的接口。
- 新添加的物理接口没有映射到兼容的模型接口。
- 未对已命名接口完成模型映射。
- 对于与其他逻辑接口（如子接口、PC 接口等）相关的接口，不进行模型映射。
- 更改某些设备型号不支持的策略或配置。例如，在接口上启用交换机端口配置。

您也可以保存带有无效模型映射的模板。但是，在设备上开始应用模板之前，您必须检查并修复模型映射。

您可以将鼠标悬停在**映射状态 (Mapping Status)** 下的**无效 (Invalid)** 上，以查看导致映射状态无效的错误。在设备上开始应用模板之前，先更正错误。

在设备模板中配置站点间 VPN 连接

具有站点间 VPN 连接的设备模板工作流程



配置 SD-WAN VPN 连接

您可以配置 SD-WAN VPN 连接，使用设备模板将分支添加到 SD-WAN 拓扑中。

开始之前

- 配置至少一个 SD-WAN 拓扑（**设备** > **VPN** > **站点间**）。
- 查看配置设备模板的前提条件和设备模板的准则和限制。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要编辑的设备模板旁边的编辑图标。

步骤 3 点击 **VPN** 选项卡。

步骤 4 点击**添加 VPN 连接 (Add VPN Connection)**。

步骤 5 从 **VPN 拓扑 (VPN Topology)** 下拉列表中选择 SD-WAN 拓扑。

系统将展开**添加 VPN 连接 (Add VPN Connection)** 对话框，在此对话框中您可以配置以下参数：

a) 从 **VPN 接口** 下拉列表中选择面向 WAN 或面向互联网的物理接口，以与中心建立 VPN 连接。此列表包含设备模板上配置的所有接口。

b) **使用 VPN 接口的 IP 地址 (Use IP Address from the VPN Interface)** - 此下拉列表使用 IP 地址变量自动填充。对于 IPv6 地址，请从下拉列表中选择 IPv6 地址。

c) 选中**本地隧道 (IKE) 身份 (Local Tunnel [IKE] Identity)** 为从分支到远程对等体的 VPN 隧道启用唯一且可配置的身份。

d) **身份类型 (Identity Type)** - 密钥 ID 是唯一支持的身份类型。从下拉列表中选择密钥 ID 变量，或点击 (+) 以创建新的密钥 ID 变量。

e) 点击**确定**。

您可以在**站点间 VPN 连接 (Site-to-Site VPN Connections)** 表中查看 VPN 连接。

步骤 6 点击**保存**。

下一步做什么

1. 在设备模板中为分支配置路由策略。
2. 将设备接口映射到模板接口（模型映射）。
3. 将模板应用到设备。

配置基于路由的站点间 VPN 连接

您可以配置基于路由的站点间 VPN 连接，使用设备模板将分支添加到基于路由的站点间 VPN 拓扑中。

开始之前

- 配置至少一个基于路由的站点间 VPN 拓扑（**设备** > **VPN** > **站点间**）。
- 查看配置设备模板的前提条件和设备模板的准则和限制。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要编辑的设备模板旁边的编辑图标。

步骤 3 点击 **VPN** 选项卡。

步骤 4 点击**添加 VPN 连接 (Add VPN Connection)**。

步骤 5 从 **VPN 拓扑 (VPN Topology)** 下拉列表中选择基于路由的站点间 VPN 拓扑。

系统将展开**添加 VPN 连接 (Add VPN Connection)** 对话框，在此对话框中您可以配置以下参数：

a) 在**虚拟隧道接口 (VTI) (Virtual Tunnel Interface [VTI])** 下拉列表中选择一个 VTI 接口，或点击 (+) 创建一个新的 VTI。

VTI 是用于建立基于路由的 VPN 隧道的虚拟接口。您必须为 VTI 配置路由策略以设置 VPN 隧道。此列表包含设备模板上配置的所有VTI。有关创建VTI的详细信息，请参阅添加VTI接口。

b) 选中**使用公共 IP 地址 (Use Public IP Address)** 复选框以覆盖隧道源 IP 地址，并为 VTI 配置公共 IP 地址变量。点击 (+) 以创建一个新的公共 IP 地址变量。

此 IP 地址是 VPN 隧道的源 IP 地址。默认情况下，这是 VPN 接口的 IP 地址。但是，如果设备位于 NAT 之后，则 VPN 接口具有专用地址，但应配置 NAT 后的公共 IP 地址。

c) 选中**本地隧道 (IKE) 身份 (Local Tunnel [IKE] Identity)** 为从分支到远程对等体的 VPN 隧道启用唯一且可配置的身份。

d) **身份类型 (Identity Type)**：密钥 ID 是唯一支持的身份类型。从下拉列表中选择密钥 ID 变量，或点击 (+) 以创建新的密钥 ID 变量。

e) （可选）选中**启用辅助 VPN 隧道 (Enable Secondary VPN Tunnel)** 复选框以配置辅助 VPN 隧道的参数。

f) 点击**确定**。

您可以在**站点间 VPN 连接 (Site-to-Site VPN Connections)** 表中查看 VPN 连接。

步骤 6 点击**保存**。

下一步做什么

1. 在设备模板中为分支配置路由策略。
2. 将设备接口映射到模板接口（模型映射）。
3. 将模板应用到设备。

配置基于策略的站点间 VPN 连接

您可以配置基于策略的站点间 VPN 连接，使用设备模板将分支添加到基于策略的站点间 VPN 拓扑中。

开始之前

- 配置至少一个基于策略的站点间 VPN (**设备** > **VPN** > **站点间**)。
- 查看配置设备模板的前提条件和设备模板的准则和限制。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要编辑的设备模板旁边的编辑图标。

步骤 3 点击 **VPN** 选项卡。

步骤 4 点击**添加 VPN 连接 (Add VPN Connection)**。

步骤 5 从 **VPN 拓扑 (VPN Topology)** 下拉列表中选择基于策略的站点间 VPN 拓扑。

系统将展开**添加 VPN 连接 (Add VPN Connection)** 对话框，在此对话框中您可以配置以下参数：

a) 从 **VPN 接口** 下拉列表中选择面向 WAN 或面向互联网的物理接口，以与中心建立 VPN 连接。

此列表包含设备模板上配置的所有接口。

执行以下操作之一来配置 VPN 接口的 IP 地址：

- 点击**使用来自 VPN 接口的 IP 地址 (Use IP Address from the VPN Interface)** 单选按钮以使用 VPN 接口的 IP 地址。

  此 IP 地址会自动填充。对于 IPv6 地址，请从下拉列表中选择 IPv6 地址。

- 点击**使用公共 IP 地址 (Use Public IP Address)** 单选按钮，为 VPN 接口配置一个公共 IP 地址。

  从下拉列表中选择 IP 地址变量，或点击 (+) 以添加 IP 地址变量。

b) 选中**本地隧道 (IKE) 身份 (Local Tunnel [IKE] Identity)** 为从分支到远程对等体的 VPN 隧道启用唯一且可配置的身份。

c) **身份类型 (Identity Type)**：密钥 ID 是唯一支持的身份类型。从下拉列表中选择密钥 ID 变量，或点击 (+) 以添加新的密钥 ID 变量。

d) **受保护的网络 (Protected Networks)**：点击 (+)，为 VPN 连接配置受保护的网络。

执行以下操作之一：

- 选择受保护的网络，然后点击**确定**。
- 点击**添加**以配置网络对象，然后点击**保存**。

  创建受保护的网络对象时，请注意以下事项：

  - 点击**主机 (Host)** 或**网络 (Network)** 单选按钮。
  - 请勿选中**允许覆盖 (Allow Overrides)** 复选框。

e) 点击**确定**。

您可以在**站点间 VPN 连接 (Site-to-Site VPN Connections)** 表中查看 VPN 连接。

步骤 6 点击**保存**。

下一步做什么

1. 请注意，在将模板应用于设备之前，要为受保护的网络配置设备特定的值，可在**模板设置 (Template Settings) > 模板参数 (Template Parameters) > 添加网络对象覆盖 (Add Network Objects Overrides)** 中添加这些对象。

2. 将设备接口映射到模板接口（模型映射）。
3. 将模板应用到设备。

使用设备模板注册设备并将其添加到基于路由的 VPN 拓扑中

本节介绍使用设备模板注册设备并将其添加到基于路由的 VPN 拓扑。

准备工作

确保拥有基于路由的 VPN 拓扑。

步骤	任务	GUI 路径	更多信息
1	创建设备模板。	设备 > 模板管理，然后点击添加设备模板	创建新设备模板，第 10 页
2	在模板中配置接口。	设备 > 模板管理，然后点击接口	编辑接口，第 13 页
3	在模板中配置基于路由的 VPN 连接。	设备 > 模板管理，然后点击 VPN > 添加 VPN 连接	配置基于路由的站点间 VPN 连接，第 23 页
4	在模板中配置路由策略。	设备 > 模板管理，然后点击路由	—
5	为模板中的设备模型添加模型映射。	设备 > 模板管理，然后点击模板设置 > 型号映射	添加模型映射，第 20 页
6	使用设备模板注册设备。	设备 > 设备管理，然后点击添加 > 设备（向导）	使用注册密钥添加设备-设备模板
7	在 VPN 拓扑的中心上部署配置。	**Deploy**	—

在双 ISP 部署中为 SD-WAN 拓扑添加设备

本节介绍在双 ISP 部署中使用设备模板将设备添加到 SD-WAN 拓扑的说明。

准备工作

确保有两个使用相同中心的 SD-WAN VPN 拓扑。有关配置 SD-WAN 拓扑的详细信息，请参阅使用 SD-WAN 向导配置 SD-WAN 拓扑。

步骤	任务	GUI 路径	更多信息
1	创建设备模板。	设备 > 模板管理	创建新设备模板，第 10 页
2	在模板中添加物理接口。 默认情况下，一个模板只有一个外部接口。重命名外部接口，例如，ISP1, ISP2。	设备 > 模板管理，然后点击接口 > 添加物理接口	添加物理接口，第 12 页
3	使用 ISP1 接口配置 SD-WAN VPN 连接。	设备 > 模板管理，然后点击 VPN > 添加 VPN 连接	配置 SD-WAN VPN 连接，第 22 页
4	使用 ISP2 接口配置 SD-WAN VPN 连接。		
5	从 ISP1 和 ISP2 接口添加静态路由到 SD-WAN 中心网络。	设备 > 模板管理，然后点击路由 > 静态路由	-
6	将 ISP1 和 ISP2 接口添加到 ECMP 区域。	设备 > 模板管理，然后点击路由 > ECMP	-
7	配置网络对象覆盖。	设备 > 模板管理，然后点击模板设置 > 模板参数 > 添加网络对象覆盖	添加网络对象覆盖，第 20 页
8	将模板接口映射到设备模型接口（模型映射）。	设备 > 模板管理，然后点击模板设置 > 型号映射	添加模型映射，第 20 页
9	将模板应用到设备。	设备 > 模板管理	应用模板，第 30 页
10	在设备上部署配置。	**Deploy**	—
11	在 SD-WAN 拓扑的中心部署配置。	**Deploy**	—

有关使用 SD-WAN 向导的双 ISP 部署的详细信息，请参阅使用 SD-WAN 向导部署双 ISP 的配置示例。

为使用数据接口管理的 设备配置模板

要配置想应用于使用 防火墙管理中心 连接的数据接口管理的 设备的模板，请确保设备的连接参数与模板匹配。这可确保威胁防御设备在应用模板后不会失去与防火墙管理中心的连接。为使用数据接口管理的 设备配置的模板不能应用于非数据接口管理的设备。

以下是连接参数列表：

- 用于管理 设备的数据接口。例如，**Ethernet1/1**。
- 接口的名称。例如，**outside**。
- 在数据接口上配置的 IP 地址。例如，DHCP 或静态 IP。
- 为数据接口配置的路由。这可以是在用于 设备与 防火墙管理中心之间的连接的数据接口上定义的默认路由或特定路由。
- 数据接口上的 DDNS 主机名配置。

如果模板上的连接参数与设备上的参数不匹配，则为确保模板成功应用于设备而进行的模板验证检查将失败。这样，模板就不会被应用到设备上。模板验证检查不会强制要求某些参数（如 IP 地址或 DDNS 主机名）完全匹配。但是，请确保配置此类参数，以便在部署后保持 设备与 防火墙管理中心 之间的连接。

以下是为确保使用数据接口管理 设备所需的配置的正确性而进行的模板验证检查列表：

- 您不能将管理器访问设备配置为管理接口的模板应用到管理器访问设备配置为数据接口的设备上。
- 您不能将管理器访问设备配置为数据接口的模板应用到管理器访问设备配置为管理接口的设备上。
- 您不能将管理器访问设备配置为单 WAN 数据接口的模板应用到管理器访问设备配置为双 WAN 数据接口的设备上。
- 如果任何连接参数不匹配，则不能将管理器访问设备配置为数据接口的模板应用到管理器访问设备配置为数据接口的设备上。

执行下面指定的程序，配置模板以使用数据接口来管理 设备。

过程

步骤 1 选择**设备** > **模板管理**。

步骤 2 点击要配置的模板的 **编辑** (✎) 图标，以使用数据接口来管理 设备。

步骤 3 点击**模板设置 (Template Settings)** 选项卡。

步骤 4 在**常规 (General)** 磁贴中，切换**按数据接口管理设备 (Manage device by Data Interface)** 按钮。

步骤 5 您将看到一个弹出窗口，要求您选择一个数据接口供管理器访问。点击**确定**。

步骤 6 点击**接口 (Interfaces)** 选项卡。

步骤 7 点击要用于管理器访问的数据界面的**编辑 (Edit)** 图标。第一个数据接口 - Ethernet1/1（外部接口）是最常用于管理器访问的数据接口。

步骤 8 在**编辑物理接口 (Edit Physical Interface)** 窗口中，点击**管理器访问 (Manager Access)** 选项卡。

步骤 9 选中**启用管理访问 (Enable management access)** 复选框。

步骤 10 点击**确定**。您将看到您选择用于管理器访问的接口已标记为**管理器访问 (Manager Access)**。

步骤 11 点击 **DHCP** 选项卡。

步骤 12 点击 **DDNS 更新方法 (DDNS Update Methods)** 选项卡。

步骤 13 点击 **+添加 (+Add)** 以添加 DDNS 更新方法。

步骤 14 在**添加 DDNS 更新方法 (Add DDNS Update Method)** 窗口中，输入**方法名称 (Method Name)**，然后选择**仅 FMC (FMC only)**。

步骤 15 根据您的要求设置**更新间隔 (Update Interval)**。

步骤 16 点击**确定**。您将在 **DDNS 更新方法 (DDNS Update Methods)** 表中看到您创建的方法。

步骤 17 点击 **DDNS 接口设置 (DDNS Interface Settings)** 选项卡。

步骤 18 点击 **+ 添加 (+Add)** 以添加动态 DNS 配置。

步骤 19 在**添加动态 DNS (Add Dynamic DNS)** 配置窗口中，选择以下字段的值：

- **接口 (Interface)** - 选择为管理器访问启用的接口
- **方法名称 (Method Name)** - 选择您创建的方法。
- **主机名 (Host Name)** - 选择主机名变量。

不要编辑此窗口中的其他字段。

步骤 20 点击**确定**。使用您创建的条目填充 **DDNS 接口设置 (DDNS Interface Settings)** 表。

步骤 21 要配置模型映射以确保模板中为管理器访问设置的数据接口与设备上为管理器访问选择的数据接口匹配，请点击**模板设置 (Template Settings)** 选项卡，然后点击**模型映射 (Model Mapping)**。

步骤 22 点击**添加模型映射 (Add Model Mapping)**。

步骤 23 从下拉列表中选择**设备模型 (Device Model)**。

步骤 24 通过从**模型接口 (Model Interface)** 下拉列表中选择接口，将模板中为管理器访问设置的日期接口映射到设备上的相应数据接口。

步骤 25 点击**保存**。接口映射会与设备模型和映射状态一起在**模型映射 (Model Mapping)** 窗口中列出。现在，您可以在使用数据接口管理的设备上应用模板。

将模板与设备一起使用

在向防火墙管理中心注册设备时，您可以选择兼容的模板进行初始配置。您也可以将模板应用于已向 防火墙管理中心 注册的设备。

使用设备模板向管理中心添加设备

您可以使用设备模板通过以下选项将设备添加到 防火墙管理中心：

- 使用注册密钥添加设备-设备模板
- 使用序列号来添加设备（零接触调配）- 设备模板

注释 任何与模板配置相关的变更管理票据都必须获得批准，才能将相应的变更纳入模板应用工作流程。在模板应用过程中，只使用已批准的模板配置。

将模板应用于现有设备

您可以将模板应用或重新应用模板到现有设备。

应用模板

您可以将模板应用于已向 防火墙管理中心注册的设备。在设备上应用模板会清除现有配置并应用模板中的配置。但是， HA 故障转移配置不会被清除。

应用模板仅会更改 防火墙管理中心 上的设备配置。您必须将这些设备配置更改显式部署到 设备上。已应用的配置更改无法回滚。但是，您也可以使用另一个模板来进行所需的配置。

注释 任何与模板配置相关的变更管理票据都必须获得批准，才能将相应的变更纳入模板应用工作流程。在模板应用过程中，只使用已批准的模板配置。

执行以下程序可在现有设备上应用模板。

过程

步骤 1 要从**模板管理**窗口应用模板，请选择**设备** > **模板管理**。

a) 点击要应用的模板旁边的 **更多** (⋮) 图标，然后点击**应用 (Apply)**。
b) 从**设备 (Device)** 下拉列表中选择要应用模板的**设备**。
c) 点击**确认 (Confirm)** 以在设备上启动模板应用。

步骤 2 （可选） 要从**关联设备 (Associated Devices)** 窗口应用模板，请依次选择**设备 (Devices)** > **模板管理 (Template Management)**。

a) 点击您要应用于设备的模板的 **编辑** (✎) 图标。
b) 点击**关联设备 (Associated Devices)**。
c) 在**关联设备 (Associated Devices)** 窗口中，点击**应用模板 (Apply Template)**。
d) 从**设备 (Device)** 下拉列表中选择要应用模板的**设备**。

e) 输入**变量**和**网络对象覆盖**字段的值。
f) 点击**应用 (Apply)** 以在设备上启动模板应用。

重新应用模板

如果对设备或模板进行了任何更改，导致配置不同步，则可以重新应用模板，使配置与模板同步。

执行以下程序在设备上重新应用模板。

过程

步骤 1 选择**设备** > **模板管理**。
步骤 2 点击您要重新应用到设备的模板的 **编辑** (✎) 图标。
步骤 3 点击**关联设备 (Associated Devices)**。
步骤 4 在**关联的设备 (Associated Devices)** 窗口中，点击要重新**应用模板 (Reapply Template)** 的设备旁边的重新应用模板。

注释
如果要在模板中的所有关联设备上重新应用模板，请点击**批量重新应用 (Bulk Reapply)**，然后点击**确认 (Confirm)**。

步骤 5 在**重新应用模板 (Reapply template)** 窗口中，您可以重复使用自动填充的**变量 (Variables)** 和**网络对象覆盖 (Network object overrides)** 值或输入新值。
步骤 6 点击**确认 (Confirm)** 以在设备上启动模板的重新应用。

监控设备模板

您可以通过查看**关联设备 (Associated Devices)** 窗口中列出的设备并查看**模板应用报告 (Template Apply Report)** 来监控和验证模板的应用情况。

查看关联设备

与模板关联的设备列在**关联设备 (Associated Devices)** 窗口中。每个设备行将显示**设备名称**、**同步状态**、**模板应用状态**和**应用日期**。您还可以点击**重新应用模板 (Reapply template)** 以重新应用模板。点击**变量摘要 (Variable Summary)** 图标以显示模板中的变量摘要，然后点击 **报告** (📋) 图标以下载设备模板应用报告。点击 **删除** (🗑) 图标从设备中删除模板。

如果要从**关联设备 (Associated Devices)** 窗口在设备上应用模板，请点击**应用模板 (Apply Template)**。如果要在模板中的所有关联设备上重新应用模板，请点击**批量重新应用 (Bulk Reapply)** ，然后点击**确认 (Confirm)**。

同步状态 (Sync Status) 可以为**同步 (Sync)** 或**不同步 (Out-of-Sync)**。如果状态显示为**同步 (Sync)**，则表示模板和设备配置相同或正在同步。如果状态显示为**不同步 (Out-of-Sync)**，则表示自上次应用模板以来，设备上或模板中的配置发生了更改。

设备与模板的关联不会因以下情况而改变：

- 设备上的待处理配置更改 - 如果设备上存在必须应用的待处理配置更改，则**同步状态**不会发生变化。
- 在设备上部署待处理配置更改 - 在设备上部署待处理配置更改后，**同步状态**不会发生变化。

下表显示了可能出现的**同步**和**不同步**场景。

在设备上应用模板后修改的设备配置	在设备上应用模板后修改的模板配置	关联状态
否	否	同步
是	否	不同步
否	是	不同步
是	是	不同步

生成模板应用报告

模板应用报告 PDF 会在模板应用任务完成后生成。无论在设备上应用模板成功还是失败，都会生成该报告。您将在**通知 (Notifications) > 任务 (Tasks)** 窗口中看到此报告的链接。

模板应用报告包含以下详细信息：

- 模板名称
- 设备型号名称
- 从其中应用模板的域
- 开始和结束时间
- 设备上的模板应用状态
- 接口映射信息
- 变量值

由于设备型号或版本不兼容，模板上的某些配置可能无法应用于设备。报告还包含有关此类配置的详细信息。报告还包含应用模板失败时遇到的任何错误。由于以下原因，在设备上应用模板可能会失败：

- 所使用的设备型号不存在型号映射。
- 变量和网络对象覆盖使用的值不符合路由策略或接口配置规则。例如，两个 IPv4 地址接口变量使用了相同的 IPv4 地址。

- 由于正在执行其他任务（如应用或修改模板），设备或模板被锁定。

审核日志

与设备模板应用、配置更新、设备模板创建和删除相关的日志记录在审计日志下。设备模板审核日志会在任务开始和结束时添加到日志中，以便在设备上应用模板。

系统还会生成一个审核差异文件，让您能够查看在设备上应用模板期间所做的配置更改。执行下面给出的程序以查看差异文件。

过程

步骤 1 选择 **系统** (⚙) > **监控** > **审核**。

步骤 2 设备模板日志记录在子系统 **设备** > **模板管理** 下。点击**差异 (diff)** 图标可打开一个新窗口，其中显示在设备上应用模板期间完成的配置更改。

设备模板故障排除

初步故障排除

要初步排除故障，我们建议查看模板应用报告中的信息，以及遇到错误时 防火墙管理中心 UI 上显示的通知。防火墙管理中心 日志文件还包含详细的调试和故障排除信息。

请按照以下步骤进行初始故障排除。

1. 检查**模板应用报告**中提到的错误。有关详细信息，请参阅模板、应用报告。
2. 查看变量值并检查重叠和不兼容情况。
3. 检查模型映射，确保是否存在正确的模型映射。相应地删除或添加映射。
4. 请参阅 防火墙管理中心 审核日志，以查找并解决任何其他问题。

请考虑以下错误场景。在设备模板中，内部接口使用静态 IPv4 变量 - *$insideIPv4* 来进行配置。

BGP IPv4 地址与 IPv4 BGP 邻居一起配置。

为 BGP 邻居和接口配置一个重叠的 IPv4 地址。

由于上述问题，设备模板的应用会失败并显示错误。

要排除此错误，请从 UI 上显示的通知中确定错误。

```
IP Address 192.168.10.1 same as ip address of interface - 'inside'(Ethernet1/1)
```

有关详细信息，请查看**模板应用报告**。

输入正确的变量值并再次应用模板，以确保在设备上成功应用模板。

设备注册故障排除

- 问题：管理员密码不正确或注册时未提供密码

  场景：如果设备上未设置管理员密码，并且您在注册时未提供管理员密码，则 设备调配将失败。在这种情况下，系统会显示调配错误和**输入密码**链接。

  解决方法：点击**输入密码**，输入新密码，然后点击**保存**。点击**确认并继续 (Confirm and Proceed)**以再次触发载入。

- 如果设备上已经设置了管理员密码，而您在注册时又提供了另一个管理员密码，则设备调配将失败。

- 问题：防火墙管理中心 中的设备注册失败

  解决方法：按照现有的设备注册故障排除步骤操作。有关详细信息，请参阅 Firepower 设备注册配置、验证和故障排除。

- 问题：在 防火墙管理中心 中的批量注册请求失败

  场景： 批量注册请求可能会在几种情况下失败：

  - 您没有执行模板相关操作所需的权限
  - 从请求域看不到模板
  - 提供的 CSV 文件无效

  解决方法：您可以在 VMS 共享和 USM 共享日志文件中看到这些错误的日志。修复错误并重新启动注册。

- 问题：由于某些一般错误（例如与设备的通信失败），安全云控制 中的设备调配失败

  解决方法：点击调配错误中的重试，以便再次触发 安全云控制 中的自行激活。您还可以参阅 安全云控制 工作流程，以了解有关错误和故障排除的更多信息。

思科安全云集成故障排除

问题：思科安全云集成不成功

解决方法：执行思科安全云集成故障排除步骤。有关详细信息，请参阅思科安全云集成。

设备模板配置问题故障排除

问题：设备模板配置错误，导致注册后部署失败

解决方法：请按照以下步骤进行初始故障排除。

1. 检查模板应用报告中提到的错误。
2. 查看变量值并检查重叠和不兼容情况。
3. 检查模型映射，确保是否存在正确的模型映射。相应地删除或添加映射。
4. 请参阅 防火墙管理中心 审核日志，以查找并解决任何其他问题。

安全云控制 问题故障排除

- 问题：已申领序列号的设备

  解决方法：验证序列号并重新启动载入。

- 问题：安全云控制 未能申领设备。

  解决方法：在 安全云控制 **安全设备 (Security Devices)** 窗口中选择设备，以了解有关错误的更多详细信息。您可以在 VMS 共享和 USM 共享日志文件中看到与设备申领问题相关的日志。点击 **重试 (Retry)** 以再次启动注册。

- 问题：防火墙管理中心 和 安全云控制 之间的通信失败

  场景：防火墙管理中心 和 安全云控制 之间的通信故障可能会导致零接触调配 (ZTP) 设备注册请求失败。

  解决方法：刷新 ZTP 设备状态，重新尝试注册 ZTP，然后再删除 ZTP 设备。您可以在身份验证后台守护程序日志中查看有关防火墙管理中心 和 安全云控制 之间通信失败的日志。对于与 ZTP 相关的操作故障，您可以查看 VMS 共享和 USM 共享日志文件中的日志。

使用设备模板进行设备管理的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
使用设备模板进行设备管理	7.6.0	7.4.1	通过设备模板，可以部署具有预配置初始设备配置的多个分支设备。您可以使用设备模板对多台设备执行批量零接触调配，对具有不同接口配置的多台设备应用 day 2 配置更改，以及从现有设备克隆配置参数。 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])** • **设备 (Devices)** > **模板管理 (Template Management)** > **添加设备模板 (Add Device Template)** • **设备 (Devices)** > **模板管理 (Template Management)** > **添加模型映射 (Add Model Mapping)** • **设备 (Devices)** > **模板管理 (Template Management)** > **编辑模板 (Edit a template)** > **模板设置 (Template Settings)** • **集成 (Integration)** > **思科安全云 (Cisco Security Cloud)**

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。