域

以下主题介绍如何使用域管理多租户：

使用域的多租户简介

管理中心 允许您使用域实施多租户。域对受管设备、配置和事件的用户访问进行分段。您在一个顶级全球域下最多可以创建 100 个子域，分为两个或三个级别。

当您登录到 管理中心时，将会登录到单个域，称为当前域。根据您的用户帐户，您或许可以切换到其他域。

除了您的用户角色所施加的任何限制之外，您当前的域级别可能也会限制您修改各样配置的能力。管理中心 会将大多数管理任务（例如系统软件更新）限制于全局域。

管理中心会限制对枝叶域（不含子域的域）的其他任务。例如，您必须将每个受管设备与一个枝叶域相关联，并从该枝叶域的情景执行设备管理任务。请注意，每台设备只能属于一个域。

根据每个枝叶域的设备收集的发现数据，该枝叶域可构建自己的网络映射。受管设备报告的事件（连接、入侵、恶意软件等）还会与设备的枝叶域相关联。

一个域级别：全局

如果不配置多租户，则所有设备、配置和事件属于全局域，其在此情景下也是一个枝叶域。除了域管理之外，系统会隐藏特定域配置和分析选项，直到您添加子域。

两个域级别：全局和第二级

在两个级别的多域部署中，全局域只有直接的后代域。例如，托管安全运营商 (MSSP) 可以使用单一 管理中心来管理多个客户的网络安全：

- MSSP 的管理员可以登录全局域，无法查看或编辑客户的部署。他们必须登录到相应的二级命名子域，才能管理客户的部署。
- 每个客户的管理员都可以登录第二级已命名子域，以便只管理适用于其组织的设备、配置和事件。这些本地管理员无法查看或影响 MSSP 的其他客户的部署。

三个域级别：全局、第二级和第三级

在三个级别的多域部署中，全局域拥有多个子域，且至少其中一个子域又拥有其自己的子域。要扩展上述示例，请考虑这样一个场景，其中一位 MSSP 客户（已经限制在一个子域中）希望进一步对其部署进行分段。此客户希望单独管理两类设备：位于网络边缘的设备，以及位于内部的设备：

- 登录到二级子域的客户的管理员无法查看或编辑客户的边缘网络部署。他们必须登录到相应的枝叶域，才能管理部署在网络边缘的设备。
- 客户边缘网络的管理员可以登录第三级（枝叶）域，以便只管理部署在网络边缘的设备，以及适用的配置和事件。同样，客户内部网络的管理员可以登录第三级域来管理内部设备、配置和事件。边缘和内部管理员无法查看彼此的部署。

注释 在使用多租户的 管理中心 中，SSO 配置只能在全局域级别应用，并且适用于全局域和所有子域。

相关主题

配置 SAML 单点登录

域术语

本文档在介绍域和多域部署时使用以下术语：

全局域

在多域部署中，是指顶级域。如果不配置多租户，则所有设备、配置和事件都属于全局域。全局域中的管理员可以管理整个 Firepower 系统部署。

子域

第二或第三级域。

第二级域

全局域的子级。第二级域可以是枝叶域，也可以具有子域。

第三级域

第二级域的子级。第三级域始终是枝叶域。

枝叶域

没有子域的域。每台设备都必须属于枝叶域。

后代域

从层次结构中的当前域下传的域。

子域

域的直接后代。

祖先域

当前域从其下传的域。

父域

域的直接祖先。

同级域

具有相同父级的域。

当前域

您现在登录的域。在 Web 界面的右上角，系统在您的用户名之前显示当前域的名称。除非您的用户角色受限，否则可以编辑当前域中的配置。

域属性

要修改域的属性，您必须在该域的父域中具有管理员访问权限。

名称和描述

每个域在层次结构中必须拥有唯一的名称。说明是可选的。

父域

第二和第三级域有父域。在创建域后，无法更改该域的父级。

设备

仅枝叶域可包含设备。换句话说，域可以包含子域或设备，但不能同时包含两者。不能保存由非枝叶域直接控制设备的部署。

在域编辑器中，Web 界面根据可用和所选设备在域层次结构中的当前位置来显示它们。

主机限制

管理中心 可以监控并因而存储在网络映射中的主机数，具体取决于其型号。在多域部署中，枝叶域共享受监控主机的可用池，但拥有单独的网络映射。

要确保每个枝叶域都可以填充其网络映射，可以在每个子域级别设置主机限制。如果将域的主机限制设置为 0，则域在通用池中共享。

设置主机限制对每个域级别有着不同的影响：

- 枝叶 - 对于枝叶域，主机限制仅是对枝叶域可以监控的主机数量进行简单限制。

- 第二级 - 对于用于管理第三级枝叶域的第二级域，主机限制表示枝叶域可以监控的主机总数。枝叶域共享可用主机池。
- 全局 - 对于全局域，主机限制等于 管理中心 可以监控的主机总数。您无法进行更改

子域的主机限制总和加起来可超过其父域的主机限制。例如，如果全局域主机限制为 150,000，则可以配置多个子域，每个子域的主机限制为 100,000。这些域中的任一个（但并非总共）可监控 100,000 台主机。

网络发现策略控制在您达到主机限制后检测到新主机时发生的情况；您可以丢弃新主机或替代非活动时间最长的主机。由于每个枝叶域具有各自的网络发现策略，因此在系统发现新主机时，每个枝叶域会监管各自的行为。

如果您降低某个域的主机限制，且其网络映射包含比新限制更多的主机，则系统会删除处于非活动状态时间最长的主机。

相关主题

Firepower 系统主机限制
网络发现数据存储设置

文件的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员

管理域

要修改域的属性，您必须在该域的父域中具有管理员访问权限。

过程

步骤 1 选择**系统**（⚙）> **域**。

步骤 2 管理域：

- 添加 - 点击**添加域 (Add Domain)**，或者点击父域旁边的**添加子域 (Add Subdomain)**；请参阅创建新域，第 5 页。

- 编辑 - 点击要修改的域旁边的**编辑**（ ），请参阅域属性，第 3 页。
- 删除 - 点击要删除的空白域旁边的**删除**（ ），然后确认您的选择。通过编辑设备的目标域移动要删除的域中的设备。

步骤 3 当您完成对域结构以及与枝叶域相关的所有设备的更改时，请点击**保存 (Save)** 以实施更改。

步骤 4 如有提示，请进行其他更改：

- 如果将枝叶域更改为父域，请移动或删除旧网络映射；请参阅在域之间移动数据，第 6 页。
- 如果在域之间移动设备，并且必须分配新的策略和安全区域或接口组，请参阅在域之间移动设备，第 6 页。

下一步做什么

- 为任何新域配置用户角色和策略（访问控制、网络发现等等）。根据需要更新设备属性。
- 部署配置更改；请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

创建新域

您在一个顶级全球域下最多可以创建 100 个子域，分为两个或三个级别。

实施域配置之前，必须将所有设备分配到枝叶域。将某个子域到枝叶域时，该域不再是枝叶域，您必须重新分配其设备。

过程

步骤 1 在全局或第二级域中，选择**系统**（ ）> **域**。

步骤 2 点击**添加域 (Add Domain)**，或者点击父域旁边的**添加子域 (Add Subdomain)**。

步骤 3 输入**名称**和**说明**。

步骤 4 在**父域 (Parent Domain)** 中选择父域。

步骤 5 在**设备 (Devices)** 上，选择**可用设备 (Available Devices)** 以添加域，然后点击**添加到域 (Add to Domain)** 或拖放到**所选设备 (Selected Devices)** 列表中。

步骤 6 或者，点击**高级 (Advanced)** 以限制新域可以监控的主机数；请参阅域属性，第 3 页。

步骤 7 点击**保存 (Save)** 返回域管理页面。

如果任何设备被分配到非枝叶域，则系统会向您发出警告。点击**创建新域 (Create New Domain)**，为这些设备创建新域。如果计划将设备移至现有域，请点击**保持未分配 (Keep Unassigned)**。

步骤 8 当您完成对域结构以及与枝叶域相关的所有设备的更改时，请点击**保存 (Save)** 以实施更改。

步骤 9 如有提示，请进行其他更改：

- 如果将枝叶域更改为父域，请移动或删除旧网络映射；请参阅在域之间移动数据，第 6 页。

- 如果在域之间移动设备，并且必须分配新的策略和安全区域或接口组，请参阅在域之间移动设备，第 6 页。

下一步做什么

- 为任何新域配置用户角色和策略（访问控制、网络发现等等）。根据需要更新设备属性。
- 部署配置更改；请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

在域之间移动数据

由于事件和网络映射与枝叶域关联，因此当您将枝叶域更改为父域时，您有两种选择：

- 将网络映射和关联事件移动到新枝叶域。
- 删除网络映射但保留事件。在这种情况下，事件仍与父域关联，直到系统根据需要或根据配置删除事件。或者，您可以手动删除旧事件。

开始之前

实施一种域配置（其中之前的枝叶域现在是父域）；请参阅管理域，第 4 页。

过程

步骤 1 对于现在为父域的每个前枝叶域：

- 选择新的**枝叶域 (Leaf Domain)** 以继承**父域 (Parent Domain)** 的事件和网络映射。
- 选择**无 (None)** 以删除父域的网络映射，但保留旧事件。

步骤 2 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

在域之间移动设备

只要源域和目标域在移动设备的域中可见，您就可以在域之间移动设备。在域之间移动设备可能会影响应用于该设备的配置和策略。在域之间移动设备时，系统会保留以下设备配置。

- 接口
- 内联集

- 路由
- DHCP
- 关联对象
- SNMP（如果可用）

在域之间移动设备时，设备的配置可能会发生以下变化：

- 如果您希望系统在将设备移动到目标域后保留设备配置，请确保：
  - 共享访问控制策略位于全局域中。我们还建议将其他共享策略放在全局域中。
- 对于 VPN 配置，
  - 站点间 VPN 配置位于目标域中。
  - 远程接入 VPN 配置和设备证书位于全局或目标域中。
  - 如果您为某一设备分配远程接入 VPN 策略，则仅当目标域是在其中配置远程接入 VPN 的域的后代时，才可以将该设备从一个域移至另一个域。
- SNMP 的网络对象位于全局域中。
- 您可以将该设备移入任何子域，而无需删除在该设备上登记的证书。具体包括：
  - 如果应用于移动设备的运行状况策略在新域中不可访问，您可以选择新的运行状况策略。
  - 如果分配给移动设备的访问控制策略在新域中无效或不可访问，请选择新策略。每个设备都必须有一个分配的访问控制策略。
  - 如果移动设备上的接口属于在新域中不可访问的安全区域，您可以选择新区域。
  - 删除以下位置中的接口：
    - 在新域中不可访问且不在访问控制策略中使用的安全区域。
    - 所有接口组。

如果设备需要策略更新，但您不需要在区域间移动设备，则系统会显示一条消息，表明区域配置为最新配置。例如，如果设备的接口属于在公共祖先域中配置的安全区域，则您无需在将设备从一个子域移动到另一个子域时更新区域配置。

开始之前

- 创建新的域。有关详细信息，请参阅创建新域，第 5 页。
- 实施您将设备从一个域移动到另一个域的域配置，且现在必须分配新策略和安全区域；请参阅管理域，第 4 页。

过程

步骤 1 在全局域中，选择**系统 (System)** (⚙) > **域 (Domains)**。

步骤 2 编辑您计划将设备移动到的目标域。

步骤 3 在**编辑域 (Edit Domain)** 对话框中，执行以下操作之一：

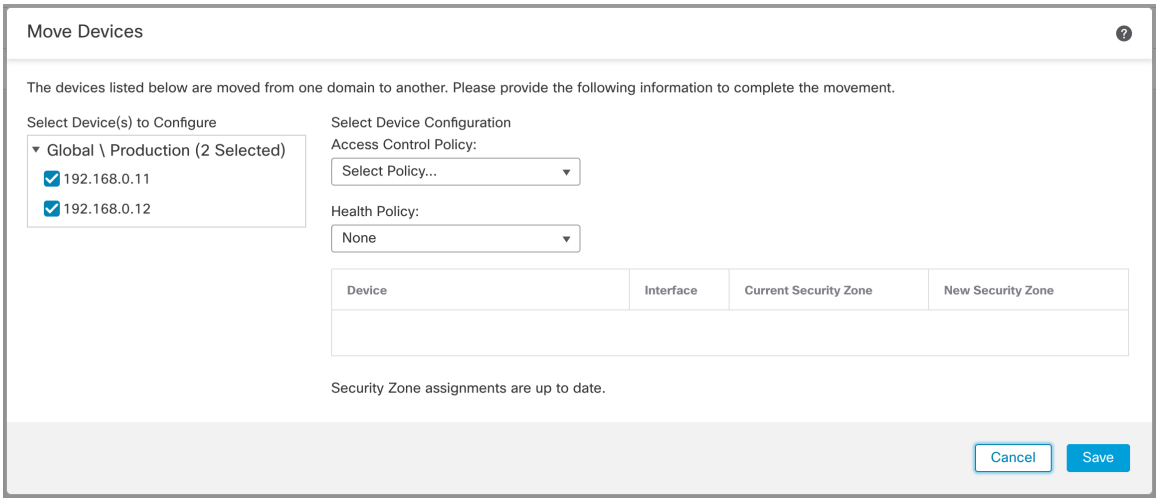
1. 选择要移动的设备，然后点击**添加到域 (Add to Domain)**。
2. 点击**保存 (Save)**。

步骤 4 在“域”(Domains) 页面上，点击**保存 (Save)**。

步骤 5 （**如果访问控制策略不在全局域中**）在**移动设备 (Move Devices)** 对话框中，执行以下操作：

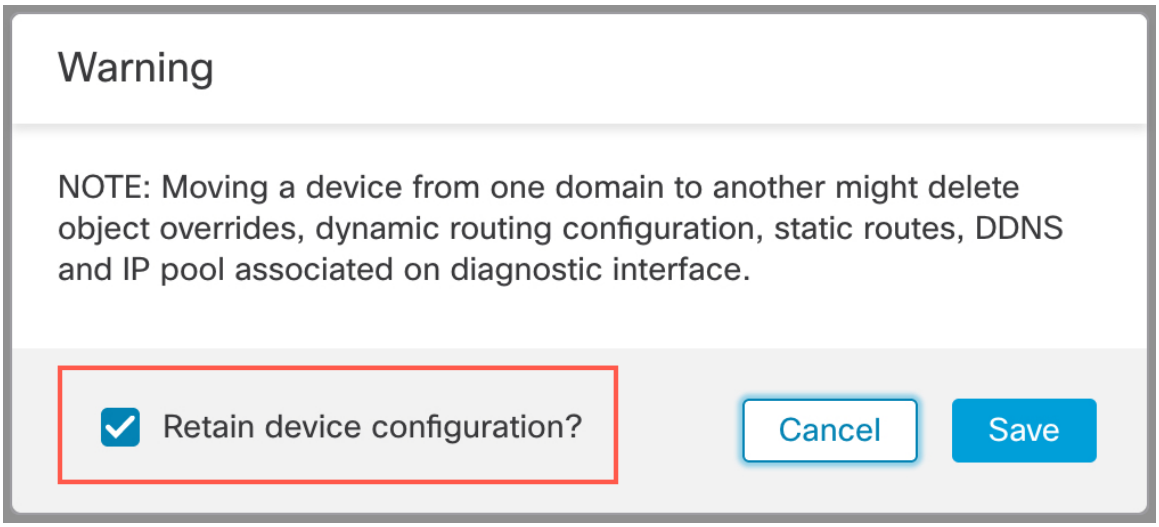
1. 在**选择要配置的设备 (Select Device(s) to Configure)** 下，选中要配置的设备。

   选中多个设备，以分配相同的运行状况和访问控制策略。



2. 在**访问控制策略 (Access Control Policy)** 中选择访问控制策略以应用于设备，或选择**新建策略 (New Policy)** 来创建新策略。
3. 在**运行状况策略 (Health Policy)** 中选择运行状况策略以应用于设备，或选择**无 (None)** 使该设备没有运行状况策略。
4. 如果系统提示将接口分配到新区域，请为列出的每个接口选择**新建安全区域 (New Security Zone)**，或选择**无 (None)** 以在稍后对其进行分配。
5. 配置完所有受影响设备后，点击**保存 (Save)**以保存策略和区域分配。

步骤 6 如果要在移动后保留设备配置，请选中**保留设备配置？(Retain device configuration?)** 复选框。



如果选择此选项，则系统会在设备被移至目标域后保留设备配置。如果不选择此选项，则您必须手动更新受移动影响的已移动设备上的设备配置。

下表显示了如何在各种场景中处理对象。

场景	系统操作
对象存在于目标域中。	重复使用对象。
目标域中存在具有相同名称和值的对象。	重复使用对象。
目标域中存在具有相同名称但值不相同的对象。	• 网络和端口 - 创建对象覆盖。 • 接口对象 - 如果类型不同，则创建新对象。 • 根据名称匹配重复使用所有其他对象类型。
对象不存在于目标域中。	创建新对象。

步骤 7 点击**保存 (Save)** 以实施域配置。

步骤 8 域配置完成后，点击**确定 (OK)**。

下一步做什么

- 在受移动影响的移动设备上更新其他配置。
- 部署配置更改；请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
- 如果在域之间移动设备后系统无法保留设备配置，则您可以手动恢复设备配置。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的导出和导入设备配置。

域管理历史记录

特性	版本	详细信息
保留与站点间 VPN 关联的设备配置	7.3	将设备从一个域移动到另一个域时，只有在目标域中配置了站点间 VPN 时，才能保留与站点间 VPN 关联的设备配置。
保留设备配置	7.2	现在，您可以在将设备从一个域移动到另一个域时保留设备配置。
增加了支持的域的最大数量	6.5	您现在最多可以添加 100 个域。以前，最大值为 50 个域。 支持的平台： Cisco Secure Firewall Management Center

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。