# 特性和功能

Firepower 版本 6.5.0包括：



# 新功能

以下主题列示了 Firepower 版本 6.5.0中可用的新功能。如果您的升级路径跳过了一个或多个主版本，请参阅思科 Firepower 发行说明查看过去的新功能列表。

## Firepower 管理中心/版本 6.5.0 中的新增功能

下表列出了在使用 Firepower 管理中心进行配置时 Firepower 版本 6.5.0 中可用的新功能：

**表 *1:* 版本 *6.5.0* 新增功能： *FMC* 部署**

| 特性 | 说明 |
|---|---|
| **硬件和虚拟硬件** | |
| Firepower 1150 上的 FTD | 我们推出了 Firepower 1150。 |
| Azure 上的更大 FTDv 实例 | Microsoft Azure 上的 Firepower 威胁防御虚拟现在支持更大的实例： D4_v2 和 D5_v2。 |
| VMware 上的 FMCv 300 | 我们推出了 FMCv 300，一个更大的 适用于 VMware 的 Firepower Management Center Virtual。与其他 FMCv 实例的 25 台设备相比，它最多可以管理 300 台设备。<br>您可以使用 FMC 模型迁移功能从功能较低的平台切换到 FMCv 300。 |

| 特性 | 说明 |
| --- | --- |
| VMware vSphere/VMware ESXi 6.7 支持 | 现在，您可以在 VMware vSphere/VMware ESXi 6.7 上部署 FMCv、FTDv 和 NGIPSv 虚拟设备。 |
| **Firepower 威胁防御** | |
| Firepower 1010 硬件交换机支持 | 现在，Firepower 1010 支持将各以太网接口设置为交换机端口或防火墙接口。<br>新增/修改的屏幕：<br>• **设备 > 设备管理 > 接口**<br>• **设备 > 设备管理 > 接口 > 编辑物理接口**<br>• **设备 > 设备管理 > 接口 > 添加 VLAN 接口**<br>支持的平台：Firepower 1010 |
| Firepower 1010 PoE + 支持以太网 1/7 和以太网 1/8 | 现在，Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。<br>新增/修改的屏幕：**设备 > 设备管理 > 接口 > 编辑物理接口 > PoE**<br>支持的平台：Firepower 1010 |
| 对运营商级 NAT 的改进。 | 对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。<br>新增/修改的屏幕： **设备** > **NAT** >添加/编辑 FTD NAT 策略>添加/编辑 NAT 规则> **PAT 池**选项卡> **块分配**选项<br>支持的平台：任何FTD设备 |

| 特性 | 说明 |
| --- | --- |
| Firepower 4100/9300 上的多个容器实例的 TLS 加密加速 | 现在，在 Firepower 4100/9300 机箱上的多个容器实例（最多16个）上支持 TLS 加密加速。以前，每个模块/安全引擎只能为一个容器实例启用 TLS 加密加速。<br>新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，使用 **create hw-crypto**和 **scope hw-crypto** CLI 命令。有关详细信息，请参阅思科 Firepower 4100/9300 FXOS 命令参考。<br>新的 FXOS CLI 命令：<br>• **create hw-crypto**<br>• **delete hw-crypto**<br>• **scope hw-crypto**<br>• **show hw-crypto**<br>删除的 FXOS CLI 命令：<br>• **show hwCrypto**（已替换为 **show hw-crypto**）<br>• **config hwCrypto**<br>删除的 FTD CLI 命令：<br>• **show crypto accelerator status**<br>支持的平台：Firepower 4100/9300 |
| **访问控制和事件分析** | |
| 访问控制规则筛选 | 现在，您可以根据搜索条件过滤访问控制规则。<br>新增/修改的屏幕：**策略 > 访问控制 > 访问控制** >添加/编辑策略> 过滤器按钮（' 仅显示符合过滤器条件的规则 '）<br>支持的平台： FMC |
| 争议 URL 类别或信誉 | 您现在可以对 URL 的类别或信誉进行争议。<br>新增/修改的屏幕：<br>• **分析 > 连接事件** >右键点击类别或信誉> **争议**。<br>• **分析 > 高级 > URL** > 搜索 URL > **争议**按钮<br>• **系统 > 集成 > 云服务 > 争议**链接<br>支持的平台： FMC |

| 特性 | 说明 |
| --- | --- |
| 使用基于目标的安全组标记（SGT）进行用户控制 | 现在，您可以在访问控制规则中将 ISE SGT 标记用于源匹配条件和目标匹配条件。SGT 标记是 ISE 获取的标签到主机/网络映射。<br>新建连接事件字段：<br>• 目标 SGT（系统日志：DestinationSecurityGroupTag）：用于连接响应方的 SGT 属性。<br>重命名连接事件字段：<br>• 目标 SGT（系统日志：SourceSecurityGroupTag）：用于连接发起方的 SGT 属性。替换安全组标记（系统日志：SecurityGroup）。<br>新增/修改的屏幕：**系统 > 集成 > 身份源 > 身份服务引擎 >**订阅**会话目录主题**和**SXP 主题**选项<br>支持的平台：任意 |
| Cisco Firepower 用户代理版本 2.5 的集成 | 我们已发布 Cisco Firepower 用户代理版本 2.5，您可以将其与 Firepower 版本 6.4.0 和 6.5.0 集成。<br>**注释** 尽管版本 6.5.0 支持它，但我们计划使用思科 Firepower 用户代理软件和身份源结束对用户控制的支持。强烈建议您立即切换到思科身份服务引擎/被动身份连接器 (ISE/ISE-PIC)。这同时使得您可以利用用户代理不可用的功能。有关详细信息，请参阅思科 Firepower 管理中心配置指南页面对应于您的版本的《思科 *Firepower* 用户代理配置指南》。<br>新增/修改的 FMC CLI 命令： **configure user-agent**<br>支持的平台： FMC |
| “数据包配置文件”CLI 命令 | 现在，您可以使用 FTD CLI 获取有关设备如何处理网络流量的统计信息。也就是说，预过滤器策略快速路径的数据包数量、作为大型流进行了卸载、完全通过访问控制（Snort）进行评估等。<br>新增的 FTD CLI 命令：<br>• **asp packet-profile**<br>• **no asp packet-profile**<br>• **show asp packet-profile**<br>• **clear asp packet-profile**<br>支持的平台： FTD |

| 特性 | 说明 |
| --- | --- |
| 思科威胁响应的其他事件类型 (CTR) | Firepower 现在可以将文件和恶意软件事件以及高优先级连接事件（即：与入侵、文件、恶意软件和安全情报事件相关的事件）发送到 CTR。<br>**注释** 对这些事件类型的支持在云中尚不可用，但很快就会出现。<br>新增/经修改的屏幕：**系统 > 集成 > 云服务**。<br>支持的平台：FTD（通过系统日志或直接集成）和经典（通过系统日志）设备 |
| **管理** | |
| 适用于 ISA 3000 设备的精确时间协议 (PTP) 配置。 | 可以使用 FlexConfig 在 ISA 3000 设备上配置精确时间协议 (PTP)。PTP 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。该协议专为工业、网络测量和控制系统而设计。<br>现在，我们允许在 FlexConfig 对象中包含 **ptp**（接口模式）命令和全局命令 **ptp mode e2etransparent** 和 **ptp domain**<br>新增/经修改的命令： **show ptp**<br>支持的平台：ISA 3000 和 FTD |
| 配置更多域（多租户） | 在实施多租户（对托管设备、配置和事件进行分段用户访问权限）时，最多可以在一个顶级全局域下以两个或三个级别创建 100 个子域。以前的最大值为 50 个域。<br>支持的平台： FMC |
| ISE 连接状态监视器增强功能 | ISE 连接状态监控运行状况模块现在会提醒您 TrustSec SXP（SGT 交换协议）订用状态的问题。<br>支持的平台： FMC |
| 区域云 | 如果您使用 Cisco 威胁响应集成、Cisco 支持诊断或 Cisco 成功网络功能，您现在可以选择区域云。默认情况下，升级会将您分配给美国（北美）区域。<br>新增/经修改的屏幕：**系统 > 集成 > 云服务**。<br>支持的平台：FMC、FTD |

| 特性 | 说明 |
| --- | --- |
| 思科支持诊断结果 | 思科支持诊断（有时称为思科主动支持）将配置和运行状况数据发送到思科，并通过我们的自动化问题检测系统处理该数据，使我们能够主动通知您的问题。在TAC情况下，此功能还允许思科TAC从您的设备收集基本信息。<br><br>在升级和重映像期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。<br><br>目前，Cisco 支持诊断支持仅限于选择平台。<br><br>新增/修改的屏幕：<br>• **系统 > 智能许可证**<br>• **系统 > 智能许可证 > 注册**<br><br>支持的平台：FMC 和托管的 Firepower 4100/9300 |
| FMC 模型迁移 | 现在，您可以使用“备份和恢复”功能在 FMC 之间（即使是不同的型号）迁移配置和事件。这使得更换FMC（由于不断增长的组织、从物理实施迁移到虚拟实施、硬件更新等技术或业务等方面的原因）变得更容易。<br><br>一般情况下，可以从低端迁移到更高端的FMC，但不能反向。不支持从 KVM 和 Microsoft Azure 迁移。您还必须在 Cisco Smart Software Manager (CSSM) 中取消注册并重新注册。<br><br>有关详细信息（包括支持的目标和目标型号），请参阅《Firepower 管理中心型号迁移指南》。<br><br>支持的平台： FMC |
| **增强安全性** | |
| 在基于 FXOS 的 FTD 设备上安全清除设备组件 | 现在，您可以使用 FXOS CLI 安全地擦除指定的设备组件。<br><br>新的 FXOS CLI 命令： **erase secure**<br><br>支持的平台：Firepower 1000/2000 和 Firepower 4100/9300 FTD 系列 |
| 在初始设置期间FMC，管理员帐户的密码要求更严格 | FMC初始设置现在要求您为管理员帐户选择 "强" 密码。设置过程会将此强密码应用于 FMC Web 界面和 CLI 管理员帐户。<br><br>**注释** 升级到版本6.5.0+不会强制您将弱密码更改为强密码。除了在物理FMC上使用LOM用户（这确实包括管理员用户），您不会被禁止选择新的弱密码。但是，我们建议所有 Firepower 用户帐户（尤其是具有管理员访问权限的用户帐户）具有强密码。<br><br>支持的平台： FMC |

| 特性 | 说明 |
| --- | --- |
| 并发用户会话限制 | 现在，您可以将可以登录的用户数量限制FMC在同一时间。您可以为具有只读角色、读/写角色或两者的用户限制并发会话。请注意，CLI 用户受读/写设置的限制。<br>新增/修改的屏幕：**系统 > 配置 > 用户配置 > 最大并发会话数允许**的选项<br>支持的平台： FMC |
| 已通过身份验证的 NTP 服务器 | 现在，您可以使用 SHA1 或 MD5 对称密钥身份验证配置 FMC 与 NTP 服务器之间的安全通信。对于系统安全，我们建议使用此功能。<br>新增/经修改的屏幕：**系统 > 配置 > 时间同步**<br>支持的平台： FMC |
| **可用性** | |
| 改进了初始配置体验 | 在新的和FMC重新映像上，向导会替换之前的初始设置过程。如果使用 GUI 向导，则在初始设置完成时，FMC 将显示 "设备管理" 页面，以便您可以立即开始许可 并设置部署。<br>设置过程还会自动安排以下各项：<br>• 软件下载。系统会创建每周计划任务，以下载（但不安装）软件补丁和适用于您的部署的公开可用的修复程序。<br>• FMC 仅配置备份。系统会创建每周计划的任务，以备份 FMC 配置并将其存储在本地。<br>• GeoDB 更新系统启用每周地理位置数据库更新。<br>这些任务计划为 UTC，这意味着在本地发生时，取决于日期和您的特定位置。此外，由于任务是以 UTC 为单位进行计划的，因此它们不会针对夏令时、夏令时或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季中的一个小时开始。<br>**注释** 我们强烈建议您查看自动计划的任务/GeoDB 更新，并根据需要进行调整。<br>升级FMC的不受影响。有关初始配置向导的详细信息，请参阅 FMC 型号的《入门指南》；有关计划任务的详细信息，请参阅《Firepower 管理中心配置指南》。<br>支持的平台： FMC |

| 特性 | 说明 |
| --- | --- |
| FMC Web 界面 Light 主题（体验） | 系统默认为经典主题，但您也可以选择实验性的 "浅色" 主题。<br>**注释** 由于光主题是实验性的，因此您可能会看到未对齐的文本或其他 UI 元素。在某些情况下，您可能还会遇到比平时慢的响应时间。如果遇到阻止您使用页面或功能的问题，请切换回经典主题。虽然我们无法对每个人作出响应，但我们也欢迎您提供反馈，请使用 "用户首选项" 页面上的反馈链接，或联系我们的 fmc-light-theme-feedback@cisco.com。<br>新增/修改的屏幕：**用户首选项**, 从您用户名下的下拉列表中<br>支持的平台： FMC |
| 查看对象的可用性增强 | 我们已增强了网络、端口、VLAN 和 URL 对象的 "查看对象" 功能，如下所示：<br>• 在访问控制策略中，在配置FTD路由时，您可以右键点击对象，然后选择 "**查看对象**" 以显示有关该对象的详细信息。<br>• 查看有关对象的详细信息时，或者当您在对象管理器中浏览对象时，点击**查找使用情况**（）现在允许您深入了解对象组和嵌套对象。<br>新增/修改的屏幕：<br>• **对象 > 对象管理**>选择支持的对象类型>**查找使用情况**（）<br>• **策略 > 访问控制 > 访问控制** >创建或编辑策略>创建或编辑规则>选择支持的条件类型>右键点击对象> **查看对象**<br>• **设备 > 设备管理** > 编辑 FTD 设备 > **路由器** > 右键点击受支持的对象 > **查看对象**<br>支持的平台： FMC |
| 部署配置更改的可用性增强功能 | 我们简化了与部署配置更改相关的错误和警告的显示。现在，您可以**点击查看所有详细**信息，而不是立即详细视图，查看有关特定错误或警告的详细信息。<br>新增/修改的屏幕： **"请求的部署的错误和警告"** 对话框<br>支持的平台： FMC |

| 特性 | 说明 |
| --- | --- |
| FTD NAT 策略管理的可用性增强功能 | 在配置 FTD NAT 时，您现在可以执行以下操作：<br>• 按设备查看NAT策略中的警告和错误。警告和错误标记出会对流量产生不利影响或阻碍策略部署的配置。<br>• 每页显示最多 1000 个 NAT 规则。默认值为 100。<br>新增/修改的屏幕：**设备 > NAT >**创建或编辑 FTD NAT 策略**> 显示每个页面**的警告和规则选项<br>支持的平台： FTD |
| **FMC REST API** | |
| 新的 REST API 功能 | 添加了以下 REST API 对象以支持版本 6.5.0 的功能：<br>• cloudregions：区域云<br>添加了以下 REST API 对象以支持较旧的功能：<br>• 类别：访问控制规则的类别<br>• 域、inheritancesettings：域和策略继承<br>• prefilterpolicies，prefilterrules，tunneltags：预过滤器策略<br>• Vlan界面： VLAN 接口<br>支持的平台： FMC |

# Firepower 设备管理器/FTD6.5.0 版本中的新增功能

**发布日期：2019 年 9 月 26 日**

下表列出了在使用 Firepower 设备管理器进行配置时 FTD 6.5.0 中可用的新功能：

| 特性 | 说明 |
| --- | --- |
| Firepower 4100/9300 的 FDM 支持。 | 现在，您可以使用 FDM 在 Firepower 4100/9300 上配置 Firepower 威胁防御。仅支持本地实例；不支持容器实例。 |
| 适用于 Microsoft Azure 云的 Firepower Threat Defense Virtual FDM 支持。 | 可以使用 Firepower 设备管理器在适用于 Microsoft Azure 云的 Firepower Threat Defense Virtual 上配置 Firepower 威胁防御。 |
| 支持 Firepower 1150。 | 我们推出了用于 Firepower 1150 的 FTD。 |

| 特性 | 说明 |
| --- | --- |
| Firepower 1010 硬件交换机支持，PoE+ 支持。 | Firepower 1010 支持将各以太网接口设置为交换机端口或常规防火墙接口。将各交换机端口分配给 VLAN 接口。Firepower 1010 还支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。<br>现在，默认配置将 Ethernet1/1 设置为外部，将 Ethernet1/2 到 1/8 设置为内部 VLAN1 接口上的交换机端口。升级至版本 6.5 将保留现有的接口配置。 |
| 接口扫描和替换。 | 接口扫描会检测机箱上的任何已添加、已删除或已恢复接口。还可以将旧接口替换为配置中的新接口，使接口无缝更改。 |
| 系统将显示经过改进的界面。 | **设备** > **接口**页面已重新组织。物理接口、桥接组、EtherChannel 和 VLAN 现有单独的选项卡。对于任何给定的设备型号，仅显示与该型号相关的那些选项卡。例如，VLAN 选项卡仅适用于 Firepower 1010 型号。此外，列表提供有关各接口配置和使用的更多详细信息。 |
| ISA 3000 新的默认配置。 | ISA 3000 默认配置已更改如下：<br>• 所有接口均是 BVI1 中的桥接组成员，未命名，因此不参与路由<br>• GigabitEthernet1/1 和 1/3 是外部接口，GigabitEthernet1/2 和 1/4 是内部接口<br>• 如果可用，则启用各内部/外部对的硬件旁路<br>• 允许从内部到外部以及从外部到内部的的所有流量<br>升级至版本 6.5 将保留现有的接口配置。 |
| 对 ASA 5515-X 的支持终止。最新支持版本为 FTD 6.4。 | 无法在 ASA 5515-X 上安装 FTD 6.5。ASA 5515-X 的最新支持版本为 FTD 6.4。 |
| 支持思科 ISA 3000 设备上访问控制规则中的通用工业协议 (CIP) 和 Modbus 应用过滤。 | 可以在思科 ISA 3000 设备上启用通用工业协议 (CIP) 和 Modbus 预处理器，并在访问控制规则中过滤 CIP 和 Modbus 应用。所有 CIP 应用名称均以“CIP”开头，例如 CIP Write。仅有一个应用适用于 Modbus。<br>要启用预处理器，必须在 CLI 会话（SSH 或控制台）进入专家模式，然后发出 **sudo /usr/local/sf/bin/enable_scada.sh {cip \| modbus \| both}** 命令。必须在每次部署后发出此命令，因为部署会关闭预处理器。 |

| 特性 | 说明 |
| --- | --- |
| 适用于 ISA 3000 设备的精确时间协议 (PTP) 配置。 | 可以使用 FlexConfig 在 ISA 3000 设备上配置精确时间协议 (PTP)。PTP 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。该协议专为工业、网络测量和控制系统而设计。<br>现在，我们允许在 FlexConfig 对象中包含 **ptp** 和 **igmp**（接口模式）命令和全局命令 **ptp mode e2etransparent** 与 **ptp domain**。我们还向 FTD CLI 添加了 **show ptp** 命令。 |
| EtherChannel（端口通道）接口。 | 可以配置 EtherChannel 接口，也称为端口通道。<br>**注释** 仅可将 FDM 中的 EtherChannel 添加至 Firepower 1000 和 2100 系列。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的 FDM **接口**页面中。<br>我们已更新**设备** > **接口**页面以允许创建 EtherChannel。 |
| 能够从 FDM 重新启动和关闭系统。 | 现在，可以从新的**重新启动/关闭**系统设置页面中重新启动或关闭系统。以前，需要通过 CLI 控制台在 FDM 中或从 SSH 或控制台会话发出 **reboot** 和 **shutdown** 命令。要使用这些命令，必须具有管理员权限。 |
| 在 FDM CLI 控制台中支持 **failover** 命令。 | 现在，可以通过 FDM CLI 控制台发出 **failover** 命令。 |
| 用于静态路由的服务级别协议 (SLA) 监控器。 | 配置服务级别协议 (SLA) 监控对象，以与静态路由配合使用。通过使用 SLA 监控，您可以跟踪静态路由的运行状况，并自动使用新路由替换故障路由。我们已将**SLA 监控器**添加至**对象**页面，并更新静态路由，以便您可以选择 SLA 监控器对象。 |

| 特性 | 说明 |
| --- | --- |
| 智能 CLI 和 FTD API 中的路由更改。 | 此版本包括对智能 CLI 和 FTD API 中的路由配置进行的一些更改。在先前版本中，存在用于 BGP 的单个智能 CLI 模板。现在，BGP（路由进程配置）和 BGP 常规设置（全局设置）有单独的模板。<br><br>在 FTD API 中，所有方法的路径均已更改，在路径中插入了“/virtualrouters”，但新的 BGP 常规设置方法除外。<br><br>• 静态路由方法路径为 /devices/default/routing/{parentId}/staticrouteentries，现在为 devices/default/routing/virtualrouters/default/staticrouteentries。<br><br>• BGP 方法分为两个新路径：/devices/default/routing/bgpgeneralsettings 和 /devices/default/routing/virtualrouters/default/bgp。<br><br>• OSPF 路径现在为 /devices/default/routing/virtualrouters/default/ospf and /devices/default/routing/virtualrouters/default/ospfinterfacesettings。<br><br>如果正在使用 FTD API 配置任何路由进程，请检查调用并在需要时更正。 |
| 新的 URL 类别和信誉数据库。 | 系统使用思科 Talos 团队提供的不同的 URL 数据库。新数据库的 URL 类别较老数据库有所不同。升级后，如有任何访问控制或 SSL 解密规则使用的类别不再存在，系统将使用相应的新类别作为替代。要使更改生效，请在升级后部署配置。待处理更改对话框将显示有关类别更改的详细信息。您可能想要检查URL过滤策略，以确认它们可继续提供所需的结果。<br><br>此外，在访问控制和 SSL 解密策略中以及**设备** > **系统设置** > **URL 过滤首选项**页面上的 URL 选项卡中添加了 URL 查找功能。此功能可用于检查分配给特定 URL 的类别。如果您对此类别持有异议，还可通过一个链接提交类别争议。使用这两项功能时您会转到一个外部网站，其中提供了有关此 URL 的详细信息。 |
| 安全情报对使用 IP 地址而不是主机名的 URL 请求使用 IP 地址信誉。 | 如果 HTTP/HTTPS 请求针对使用 IP 地址而不是主机名的 URL，则系统会在网络地址列表中查找IP地址信誉。无需在网络和URL列表中复制IP地址。这使得最终用户难以使用代理来避免安全情报信誉阻止。 |

| 特性 | 说明 |
| --- | --- |
| 支持向思科云发送连接和高优先级入侵、文件和恶意软件事件。 | 可以将事件发送至思科云服务器。各种思科云服务均可从这里访问事件。然后，可以使用这些云应用（例如思科威胁响应）来分析事件并评估设备可能遇到的威胁。启用该服务后，设备将向思科云发送连接和高优先级入侵、文件和恶意软件事件。<br>我们已将**设备** > **系统设置** > **云服务**上的思科威胁响应项目重命名为“将事件发送至思科云”。 |
| 思科云服务区域支持。 | 系统现在要求在注册智能许可时选择思科云区域。此区域用于思科防御协调器、思科威胁响应、思科成功网络和任何通过思科云的云功能。如果从先前的版本升级已注册设备，则会自动分配至US区域；如果需要更改区域，则必须注销智能许可，然后重新注册并选择新区域。<br>我们已在“智能许可证”页面和“初始设备设置向导”中的许可证注册流程中添加一步。您还可以在**设备** > **系统设置** > **云服务**页面上查看该区域。 |
| FTD REST API 版本 4 (v4)。 | 适用于软件版本 6.5 的 FTD REST API 已升级到第 4 版。必须将 API URL 中的第 1 版/第 2 版/第 3 版替换为第 4 版。第 4 版 API 包括许多涵盖软件版本 6.5 中添加的所有功能的新资源。请重新评估所有现有的调用，因为正在使用的资源型号可能已发生更改。要打开 API Explorer，以便在其中查看这些资源，请登录 FDM，然后点击更多选项按钮 ( ⋮ ) 并选择 **API Explorer**。 |

| 特性 | 说明 |
| --- | --- |
| FTD API 支持 TrustSec 安全组作为访问控制规则中的源和目的地匹配条件。 | 可以使用 FTD API 配置访问控制策略规则，将 TrustSec 安全组用于源或目的地流量匹配条件。系统从 ISE 下载安全组标记 (Sgt) 的列表。可以将系统配置为侦听 SXP 更新，以获取静态 SGT 到 IP 地址映射。<br><br>可以使用 GET/object/securitygrouptag 方法查看已下载标记列表，并使用 SGTDynamicObject 资源为一个或多个标记创建动态对象。这是动态对象，可在访问控制规则中用于定义基于源或目的安全组的流量匹配条件。<br><br>请注意，如果在 FDM 中编辑这些对象，则会保留对 ISE 对象或与安全组相关的访问控制规则所做的任何更改。但是，如果在 FDM 中编辑规则，则无法在该访问规则中看到安全组条件。如果使用 API 配置基于安全组的访问规则，随后使用 FDM 编辑访问控制策略中的规则时，请小心。<br><br>我们添加或修改了以下 FTD API 资源：AccessRule（SourceDynamicObjects 和 destinationDynamicObjects 属性）、IdentityServicesEngine（SubscribeToSessionDirectoryTopic 和 subscribeToSxpTopic 属性）、SecurityGroupTag 和 SGTDynamicObject。<br><br>我们在事件查看器中添加源和目的安全组标记，并将其命名为列。 |
| 使用 FTD API 导入/导出配置。 | 可以使用 FTD API 导出设备配置和导入配置文件。可以编辑配置文件以更改值，例如分配给接口的 IP 地址。因此，可以使用导入/导出创建用于新设备的模板，以便快速应用基线配置并更快地在线获取新设备。还可以使用导入/导出在重新映像设备后恢复配置。或者，还可以用它将一组网络对象或其他项目分发至一组设备。<br><br>我们添加了 ConfigurationImportExport 资源和方法（/action/configexport、/jobs/configexportstatus、/action/downloadconfigfile、/action/uploadconfigfile、/action/configfiles、/action/configimport 和 /jobs/configimportstatus）。 |
| 创建和选择自定义文件策略。 | 可以使用 FTD API 创建自定义文件策略，然后使用 FDM 选择访问控制规则的这些策略。<br><br>我们添加了以下 FTD API FileAndMalwarePolicies 资源：filepolicies、filetypes、filetypecategories、ampcloudconfig、ampservers 和 ampcloudconnections。<br><br>还删除了两个预定义策略，“阻止 Office 文档和 PDF 上传，阻止其他恶意软件”和“阻止 Office 文档上传，阻止其他恶意软件”。如果使用这些策略，则会在升级期间转换为用户定义策略，以便可以对其进行编辑。 |

| 特性 | 说明 |
| --- | --- |
| 采用 FTD API 的安全情报 DNS 策略配置。 | 可以使用 FTD API 配置安全情报 DNS 策略。此策略不会显示在 FDM 中。<br><br>我们添加了以下 SecurityIntelligence 资源：domainnamefeeds、domainnamegroups、domainnamefeedcategories 和 securityintelligencednspolicies。 |
| 使用 Duo LDAP 进行远程接入 VPN 双因素身份验证。 | 可以将 Duo LDAP 配置为远程接入 VPN 连接配置文件的第二个身份验证源，以使用 Duo 密码、推送通知或电话呼叫提供双因素身份验证。虽然必须使用 FTD API 创建 Duo LDAP 身份源对象，但可以使用 FDM 选择该对象作为 RA VPN 连接配置文件的身份验证源。<br><br>我们向 FTD API 添加了 duoldapidentitysources 资源和方法。 |
| FTD API 支持用于授权远程接入 VPN 连接的 LDAP 属性映射。 | 可以使用自定义 LDAP 属性映射增加远程接入 VPN 的 LDAP 授权。LDAP 属性映射会将客户特定的 LDAP 属性名称和值等同于思科属性名称和值。可以使用这些映射根据 LDAP 属性值将组策略分配给用户。仅可使用 FTD API 配置这些映射；无法使用 FDM 对其进行配置。但是，如果使用 API 设置这些选项，则随后可在 FDM 中编辑 Active Directory 身份源，并保留您的设置。<br><br>我们添加或修改了以下 FTD API 对象模型：LdapAttributeMap、LdapAttributeMapping、LdapAttributeToGroupPolicyMapping、LDAPRealm、LdapToCiscoValueMapping、LdapToGroupPolicyValueMapping 和 RadiusIdentitySource。 |
| FTD API 支持站点间 VPN 连接反向路由注入和安全关联 (SA) 生存期。 | 可以使用 FTD API 启用站点间 VPN 连接反向路由注入。通过反向路由注入 (RRI)，静态路由能够自动插入到受远程隧道终端保护的网络和主机的路由进程中。默认情况下，启用配置连接时添加路由的静态 RRI。动态 RRI（仅在建立安全关联 [SA] 时才会插入路由，且在 SA 断开时予以删除）会被禁用。请注意，动态 RRI 仅支持 IKEv2 连接。<br><br>还可以设置连接的安全关联 (SA) 生存期（传输的秒数或千字节数）。还可以设置无限生存期。默认生命周期是 28800 秒（八小时）和 4608000 千字节（传输一小时，每秒钟 10 兆字节）。达到生存期后，终端会协商新的安全关联和密钥。<br><br>无法使用 FDM 配置这些功能。但是，如果使用 API 设置这些选项，则随后可在 FDM 中编辑连接配置文件，并保留您的设置。<br><br>我们已将以下属性添加至 SToSConnectionProfile 资源：dynamicRRIEnabled、ipsecLifetimeInSeconds、ipsecLifetimeInKiloBytes、ipsecLifetimeUnlimited 和 rriEnabled。 |

| 特性 | 说明 |
| --- | --- |
| 在 IKE 策略中支持 Diffie-hellman 组 14、15 和 16。 | 现在，可以将 IKEv1 策略配置为使用 DH 组 14，将 IKEv2 策略配置为使用 DH 组 14、15 和 16。如果使用 IKEv1，请将所有策略升级到 DH 组 14，因为未来版本中将删除组 2 和组 5。此外，应该避免在 IKEv2 策略中使用 DH 组 24，避免在任何 IKE 版本中使用 MD5，因为未来版本中也会删除这些组。 |
| 部署更改时的性能改进。 | 如果添加、编辑或删除访问控制规则，则系统已得到增强，部署更改的速度比先前版本更快。<br>对于在用于故障切换的高可用性组中配置的系统，将已部署更改同步至备用设备的过程已得到改进，从而加快同步速度。 |
| 改进了系统控制面板上 CPU 和内存使用情况的计算方法。 | 计算 CPU 和内存使用情况的方法已得到改进，使得系统控制面板上显示的信息能够更准确地反映设备的实际状态。 |
| 升级至 FTD 6.5 后，系统不再提供历史报告数据。 | 将现有系统升级至 FTD 6.5 时，由于数据库架构发生变化，历史报告数据将不可用。因此，升级前，在控制面板中将不会看到使用情况数据。 |

# 已弃用的功能

本主题按 Firepower 版本列示了弃用的功能和平台。如果您的升级路径跳过了一个或多个主版本，必须查看中间版本的信息。

有关所有受支持的 Firepower 版本的详细兼容性信息，包括弃用平台的销售终止和生命周期终止公告的链接，请参阅思科 Firepower 兼容性指南。

### 版本 6.5.0 弃用的功能

这些功能在版本 6.5.0 中被弃用。

**注释** 尽管版本 6.5.0 支持它，但我们计划使用思科 Firepower 用户代理软件和身份源结束对用户控制的支持。强烈建议您立即切换到思科身份服务引擎/被动身份连接器 (ISE/ISE-PIC)。这同时使得您可以利用用户代理不可用的功能。有关详细信息，请参阅思科 Firepower 管理中心配置指南页面对应于您的版本的《思科 *Firepower* 用户代理配置指南》。

表 *2:* 版本 *6.5.0* 弃用的功能

| 特性 | 说明 |
| --- | --- |
| 禁用 FMC CLI 的能力 | 版本 6.3.0 中引入了 FMC CLI，您必须明确启用它。版本 6.5.0 会为新部署和升级的部署自动启用 FMC CLI。如果要访问 Linux 外壳程序（亦称为专家模式），必须登录到 CLI，然后使用 **expert** 命令。<br>注意　我们强烈建议您不要使用外壳程序访问 Firepower 设备，除非思科 TAC 让您这样做。<br>弃用的选项：**System > Configuration > Console Configuration > Enable CLI access** 复选框 |
| TLS 1.0 & 1.1 | 要增强安全性，请执行以下操作：<br>• 强制网络门户（主动身份验证）已删除对 TLS 1.0 的支持。<br>• 主机输入已删除对 TLS 1.0 和 TLS 1.1 的支持。<br>如果您的客户端无法与 Firepower 设备连接，我们建议您升级客户端以支持 TLS 1.2。 |
| 适用于 Firepower 4100/9300 的 TLS 加密加速 FXOS CLI 命令 | 作为允许在 Firepower 4100/9300 上为多个容器实例执行 TLS 加密加速的一部分，我们删除了以下 FXOS CLI 命令：<br>• **show hwCrypto**<br>• **config hwCrypto**<br>并添加了以下 FTD CLI 命令：<br>• **show crypto accelerator status**<br>有关替换的详细信息，请参阅新功能文档。 |
| 思科安全数据包分析器集成 | 版本 6.5.0 不再支持 FMC 与思科安全数据包分析器集成。<br>弃用的屏幕/选项：<br>• **System > Integration > Packet Analyzer**<br>• **Analysis > Advanced > Packet Analyzer Queries**<br>• 右键单击仪表板或事件查看器中的事件时 **Query Packet Analyzer** |
| Firepower 管理中心型号 MC750、1500 和 3500 | 不能在型号 MC750、MC1500 和 MC3500 上升级到或全新安装版本 6.5.0+ 的 Firepower 管理中心软件。不能利用这些 FMC 管理版本 6.5.0+ 的设备。 |

| 特性 | 说明 |
| --- | --- |
| 安装了 Firepower 软件的 ASA 5515-X 和 ASA 5585-X 系列设备 | 不能在这些型号上升级或全新安装版本 6.5.0+ 的 Firepower 软件（包括 FTD 和 ASA FirePOWER）：<br>• ASA 5515-X<br>• ASA 5585-X-SSP-10、-20、-40、-60<br>但是，您可以通过版本 6.5.0 的 FMC 管理较旧的设备（版本 6.2.3 至 6.4.x）。 |
| Firepower 7000/8000 系列设备 | 不能在 Firepower 7000/8000 系列设备（包括 AMP 型号）上升级或全新安装版本 6.5.0+ 的 Firepower 软件：但是，您可以通过版本 6.5.0 的 FMC 管理较旧的设备（版本 6.2.3 至 6.4.x）。 |

### 版本 6.4.0 弃用的功能

这些功能在版本 6.4.0 中被弃用。

表 *3:* 版本 *6.4.0* 弃用的功能

| 特性 | 说明 |
| --- | --- |
| SSL 硬件加速 FTD CLI 命令 | 作为 TLS 加密加速功能的一部分，我们删除了以下 FTD CLI 命令：<br>• **system support ssl-hw-accel enable**<br>• **system support ssl-hw-accel disable**<br>• **system support ssl-hw-status**<br>有关替换的详细信息，请参阅新功能文档。 |

### 版本 6.3.0 弃用的功能

这些功能在版本 6.3.0 中被弃用。

表 *4:* 版本 *6.3.0* 弃用的功能

| 特性 | 说明 |
| --- | --- |
| EMS 对于解密的扩展支持（仅 6.3.0） | 版本 6.3.0 不再提供 EMS 扩展支持，版本 6.2.3.8/6.2.3.9 中引入了此支持。这意味着**解密 - 重新签名**及**解密 - 已知密钥** SSL 策略操作在 ClientHello 协商期间不再支持有助实现更安全通信的 EMS 扩展。EMS 扩展由 RFC 7627 定义。<br>在FMC部署中，此功能取决于设备版本。只要设备运行支持的版本，将 FMC 升级到版本 6.3.0 就不会造成支持中断。但是，将设备升级到版本 6.3.0 会导致支持中断。<br>版本 6.3.0.1 中重新提供支持。 |
| 无源和内联分流接口的解密 | 版本6.3.0不再支持在无源或内联分流模式下解密接口上的流量，即使 GUI 允许您这样配置也不例外。对加密流量的任何检查都必须受到限制。 |
| VMware 5.5 托管 | 尚未在 VMware vSphere/VMware ESXi 5.5 上测试版本 6.3.0+ 的虚拟部署。我们建议您在升级 Firepower 软件之前升级托管环境。 |
| 安装了 Firepower 软件的 ASA 5506-X 系列和 ASA 5512-X 设备 | 不能在这些型号上升级或全新安装版本 6.3.0+ 的 Firepower 软件（包括 FTD和 ASA FirePOWER）：<br>• ASA 5506-X、5506H-X、5506W-X<br>• ASA 5512-X<br>但是，您可以通过版本 6.3.0 的 FMC 管理较旧的设备（版本 6.1.0 至 6.2.3.x）。 |

# 弃用的 FlexConfig 命令

某些 Firepower 威胁防御功能需使用 ASA 配置命令进行配置。从版本 6.2（FMC 部署）或版本 6.2.3（FDM 部署）开始，您可以使用 Smart CLI 或 FlexConfig 手动配置 Web 界面中不支持的各种 ASA 功能。

FTD升级可以为先前使用 FlexConfig 配置的功能添加 GUI 或 Smart CLI 支持。这可以弃用您当前使用的 FlexConfig 命令。虽然现有配置仍然有效，且仍然可以部署，但无法使用新近弃用的命令分配或创建 FlexConfig 对象。

升级后，检查 FlexConfig 策略和对象。如果有任何对象包含已被弃用的命令，则消息会指出问题所在。我们建议您重新进行配置。对新配置感到满意后，可以删除有问题的 FlexConfig 对象或命令。

### 使用 Firepower 管理中心的 FTD

此表列示了已弃用的 FlexConfig 对象及其关联的文本对象。有关预定义对象的完整列表，请参阅《Firepower 管理中心配置指南》。

表 5: 使用 FMC 的 FTD：弃用的 FlexConfig 对象

| 弃用 | 对象 | 详细信息 | 新建地点 |
|---|---|---|---|
| 6.3.0+ | FlexConfig 对象：<br>• Default_DNS_Configure<br>关联的文本对象：<br>• defaultDNSNameServerList<br>• defaultDNSParameters | 配置默认 DNS 组，该组定义在数据接口上解析完全限定域名时可以使用的 DNS 服务器。这使您可以使用 CLI 中的命令（如 **ping**），并且使用主机名而不是 IP 地址。 | 在 FTD平台设置策略中为数据接口配置 DNS。 |
| 6.3.0+ | FlexConfig 对象：<br>• TCP_Embryonic_Conn_Limit<br>• TCP_Embryonic_Conn_Timeout<br>关联的文本对象：<br>• tcp_conn_misc<br>• tcp_conn_limit<br>• tcp_conn_timeout | 配置初始连接限制和超时以防止 SYN 洪流拒绝服务 (DoS) 攻击。 | 在 FTD服务策略中配置这些功能，您可以在分配给设备的访问控制策略的 Advanced 选项卡上找到该策略。 |

此表列示了版本 6.2.3+ 中为使用 FDM 的 FTD 新近弃用的 CLI 命令。有关弃用命令的完整列表，包括在版本 6.2.0 中引入功能时弃用的命令，请参阅《Firepower 管理中心配置指南》。

表 6: 使用 FMC 的 FTD：弃用的 CLI 命令

| 弃用 | 命令 | 详细信息 |
|---|---|---|
| 6.2.3+ | **pager** | 阻止配置。 |

### 使用 Firepower 设备管理器的 FTD

此表列示了版本 6.3.0+ 中为使用 FDM 的 FTD 新近弃用的 CLI 命令。有关弃用命令的完整列表，包括在版本 6.2.3 中引入功能时弃用的命令，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。

表 7: 使用 FDM 的 FTD：弃用的 CLI 命令

| 弃用 | 命令 | 详细信息 |
|---|---|---|
| 6.3.0+ | **access-list** | 不能再创建 **extended** 和 **standard** 访问列表。使用智能 CLI 扩展访问列表或标准访问列表对象创建这些 ACL。然后，可以在按对象名称引用 ACL 且支持 FlexConfig 的命令中使用，例如带扩展 ACL 的 **match access-list** 用于服务策略流量类别。 |

| 弃用 | 命令 | 详细信息 |
|---|---|---|
| 6.3.0+ | **as-path** | 创建智能 CLI AS 路径对象，并将其用于智能 CLI BGP 对象，以配置自治系统路径过滤器。 |
| 6.3.0+ | **community-list** | 创建智能 CLI 扩展社区列表或标准社区列表对象，并将其用于智能 CLI BGP 对象，以配置社区列表过滤器。 |
| 6.3.0+ | **dns-group** | 使用 **Objects** > **DNS Groups** 配置 DNS 组，并使用 **Device** > **System Settings** > **DNS Server** 分配这些组。 |
| 6.3.0+ | **policy-list** | 创建智能 CLI 策略列表对象，并将其用于智能 CLI BGP 对象，以配置策略列表。 |
| 6.3.0+ | **prefix-list** | 创建智能 CLI IPv4 前缀列表对象，并将其用于智能 CLI OSPF 或 BGP 对象，以配置 IPv4 前缀列表过滤。 |
| 6.3.0+ | **route-map** | 创建智能 CLI 路由映射对象，并将其用于智能 CLI OSPF 或 BGP 对象，以配置路由映射。 |
| 6.3.0+ | **router bgp** | 使用适用于 BGP 的 Smart CLI 模板。 |

# FMC 菜单更改

此表列示了更改后的Firepower管理中心菜单（页面更改）。有关新增和删除的菜单选项，请参阅新功能和弃用功能文档。

表 *8: Firepower* 管理中心菜单更改

| 版本 | 新菜单路径 | 旧菜单路径 |
|---|---|---|
| 6.4.0 | **System** > **Integration** > **Cloud Services** | **System** > **Integration** > **Cisco CSI** |
| 6.3.0 | **Analysis > Lookup > Whois** | **Analysis > Advanced > Whois** |
| 6.3.0 | **Analysis > Lookup > Geolocation** | **Analysis > Advanced > Geolocation** |
| 6.3.0 | **Analysis > Lookup > URL** | **Analysis > Advanced > URL** |
| 6.3.0 | **Analysis > Custom > Custom Workflows** | **Analysis > Advanced > Custom Workflows** |
| 6.3.0 | **Analysis > Custom > Custom Tables** | **Analysis > Advanced > Custom Tables** |
| 6.3.0 | **Analysis > Vulnerabilities > Vulnerabilities** | **Analysis > Hosts > Vulnerabilities** |
| 6.3.0 | **Analysis > Vulnerabilities > Third-Party Vulnerabilities** | **Analysis > Hosts > Third-Party Vulnerabilities** |

# FMC 操作方法演练

版本 6.3.0 引入 FMC 上的演练（也称为使用方法），该演练将指导您完成各种基本任务，例如设备设置和策略配置。仅需单击浏览器窗口底部的**使用方法**，选择某一演练，然后按照分步说明进行操作。

**注释** 演练已在 Firefox 和 Chrome 浏览器上进行了测试。如果您在使用其他浏览器时遇到问题，我们会要求您切换到 Firefox 或 Chrome。如果问题持续存在，请联系 Cisco TAC。

下表列出了一些常见的问题和解决方案。要在任何时候结束演练，请单击右上角的 **x** 。

**表 *9:* 故障排除演练**

| 问题 | 解决方案 |
| --- | --- |
| 找不到**使用方法**链接来启动演练。 | 请确保演练已启用。在用户名下面的下拉列表中，选择**用户首选项**，然后单击**方法设置**。 |
| 当您不期望时，系统会显示演练。 | 如果在您不期望的情况下出现本演练， 会结束本演练。 |
| 演练会突然消失或退出。 | 如果演练消失，请执行以下操作：<br>• 移动指针。<br>有时，FMC 会停止显示正在进行的演练。例如，指向不同的顶级菜单可以实现这种情况。<br>• 导航到其他页面，然后重试。<br>如果移动指针不起作用，则本演练可能会退出。 |
| 演练与 FMC 不同步：<br>• 从错误的步骤开始。<br>• 过早进行。<br>• 不会进行。 | 如果演练不同步，您可以执行以下操作：<br>• 尝试继续。<br>例如，如果在字段中输入的值无效，并且 FMC 显示错误，则演练可能会提前进行。您可能需要返回并解决该错误以完成任务。<br>• 结束本演练，导航至其他页面，然后重试。<br>有时，您无法继续。例如，如果在完成某一步后未单击**下一步**，则可能需要结束本演练。 |