许可证

本章提供有关不同许可证类型、服务订用、许可要求等的深入信息。

注释 防火墙管理中心 支持智能许可证或旧版 PAK（产品激活密钥）许可证作为其平台许可证。有关使用 PAK 许可证的更多信息，请参阅 配置防火墙管理中心基于 PAK 的旧版许可证， 第 47 页。

关于许可证

思科智能许可是一种灵活的许可模式，为您提供一种更简便、更快速、更一致的方式来购买和管理整个思科产品组合和整个组织中的软件。此外它很安全，您可以控制用户可访问的内容。借助智能许可，您可以：

- **轻松激活：** 智能许可建立了可在整个组织中使用的软件许可证池，不再需要产品激活密钥 (PAK)。
- **统一管理：** 利用 My Cisco Entitlements (MCE)，您可以在一个易于使用的门户中全面了解您的所有 Cisco 产品和服务，始终了解您拥有以及正在使用的产品和服务。
- **许可证灵活性：** 您的软件没有与硬件节点锁定，因此您可以根据需要轻松使用和传输许可证。

要使用智能许可，您必须先在 Cisco Software Central (software.cisco.com) 上创建智能帐户。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

智能软件管理器和账户

当购买一个或多个许可证时，您可在智能软件管理器中对其进行管理： https://software.cisco.com/#module/SmartLicensing。通过思科智能软件管理器，您可以为组织创建一个主账户。如果您还没有账户，请点击此链接以设置新账户。通过思科智能软件管理器，您可以为组织创建一个主账户。有关说明，请参阅创建思科账户。

默认情况下，许可证分配给主账户下的默认虚拟帐户。作为账户管理员，您可以创建其他虚拟帐户；例如，为区域、部门或子公司创建账户。使用多个虚拟账户有助于管理大量许可证和设备。

您可以通过虚拟账户管理许可证。只有该虚拟账户的设备可以使用分配给该账户的许可证。如果您需要其他许可证，则可以从另一个虚拟账户传输未使用的许可证。您还可以在虚拟账户之间迁移设备。

气隙部署的许可选项

下表比较对无互联网访问环境中的许可部署可用的选项。对于您面临的具体情况，您的销售代表可能会提供其他建议。

表 *1:* 气隙网络许可选项的比较

智能软件管理器本地版	特定许可证预留
可对大量产品进行扩展	最适合少量设备
自动化许可管理、使用情况和资产管理可视性	有限的使用情况和资产管理可视性
添加设备不会增加运营成本	添加设备的运营成本随时间推移呈线性增长
灵活、易用、开销更低	移动、添加和更改的管理和手动开销较大
允许初期和各类到期状态下存在不合规状态	不合规状态影响系统运作
有关详细信息，请参阅将防火墙管理中心注册到本地智能软件管理器，第 28 页	有关详细信息，请参阅配置特定许可证预留 (SLR)，第 36 页

管理中心和设备的许可工作原理

防火墙管理中心 向智能软件管理器注册，然后为每个受管设备分配许可证。设备不直接向智能软件管理器注册。

物理 防火墙管理中心 本身不需要许可证。 Firewall Management Center Virtual 需要平台许可证。

与智能软件管理器的定期通信

为维护产品许可证授权，您的产品必须与智能软件管理器定期通信。

您可以使用产品实例注册令牌通过思科智能软件管理器注册 防火墙管理中心。智能软件管理器会为 防火墙管理中心 和智能软件管理器之间的通信颁发 ID 证书。此证书有效期为 1 年，但需要每 6 个月续签一次。如果 ID 证书到期（一年后没有通信）， 防火墙管理中心 可能会从您的账户中删除。

防火墙管理中心 定期与智能软件管理器通信。如果您在智能软件管理器中进行更改，则可以刷新 防火墙管理中心上的授权，以使更改立即生效。另外，也可以等待 防火墙管理中心 按计划通信。

您的 防火墙管理中心 必须具有对智能软件管理器的直接互联网访问权限，或使用气隙部署的许可选项， 第 2 页中所述的选项之一。在 non-airgapped 部署中，常规许可证通信每 30 天进行一次，但如果具有宽限期，则 防火墙管理中心 会最多运行 90 天，而不会联系智能软件管理器。确保 防火墙管理中心 在 90 天内联系智能软件管理器，否则 防火墙管理中心 将恢复为未注册状态。

评估模式

在 防火墙管理中心 向智能软件管理器注册之前，它会在评估模式下运行 90 天。您可以将功能许可证分配给受管设备，它们将在评估模式的持续时间内保持合规。此时间段结束后， 防火墙管理中心 将取消注册。

如果您向智能软件管理器注册 防火墙管理中心 ，则评估模式将结束。如果您稍后取消注册 防火墙管理中心，则无法恢复评估模式，即使最初没有使用所有 90 天。

有关未注册状态的详细信息，请参阅已注销状态， 第 4 页。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

注释 安全防火墙版本 7.6.0 中评估模式的 Talos 证书设置为 2025 年 3 月 31 日到期。在此日期之后，将停止在评估模式下访问 Talos 托管的服务（特别是与网络信誉/分类查找相关的服务）。

不合规状态

防火墙管理中心 在以下情况下可能会处于不合规状态：

- 过度使用 - 当托管设备或 Firewall Management Center Virtual 使用不可用的许可证时。

注释 即使设备的一个许可证不可用，防火墙管理中心也会处于**不合规**状态。所有配置的部署都将正常工作。例如，有两个恶意软件许可证和三个托管设备。所有三个设备都将处于**不合规**状态，并且恶意软件功能将无法工作。此行为适用于所有许可证。

- 许可证到期 - 当托管设备基于时间的许可证到期时。

在不合规状态下，请参阅以下影响：

- Firewall Management Center Virtual 平台许可证 - 操作不受影响。
- 所有 托管设备许可证 - 操作不受影响。

在您解决许可问题后，防火墙管理中心将显示它现在符合智能软件管理器的定期计划授权。要强制授权，请点击 **系统** (⚙) > **许可证** > **智能许可证** 页面上的 **重新授权** 。

已注销状态

在以下情况下， 防火墙管理中心 可能会取消注册：

- 评估模式到期-评估模式在 90 天后到期。
- 手动注销 防火墙管理中心
- 与智能软件管理器缺少通信- 防火墙管理中心 在 1 年内不与智能软件管理器通信。注意：90 天后，防火墙管理中心 授权将到期，但可以在一年内成功恢复通信，以自动重新授权。一年后，ID 证书到期，将从您的账户中删除 防火墙管理中心 ，因此您必须手动重新注册 防火墙管理中心。

在未注册状态下， 防火墙管理中心 无法将任何配置更改部署到 需要许可证的功能的设备。

最终用户许可证协议

http://www.cisco.com/go/softwareterms 提供了用于监管您使用此产品的思科最终用户许可证协议 (EULA) 和所有适用补充协议 (SEULA)。

许可证类型和限制

本节介绍可用的许可证类型。

表 *2:* 智能许可证

您分配的许可证	持续时间	授予的功能
基础版	永久或订用 **注释** 基础版 订用许可证仅在 Firewall Threat Defense Virtual上受支持。	除特定许可证预留和 Cisco Secure Firewall 3100/4200、 永久许可证会自动分配给所有 。基础版 用户和应用控制 交换和路由 NAT 有关详细信息，请参阅基础版许可证 ， 第 6 页。

您分配的许可证	持续时间	授予的功能
IPS	订用	入侵检测和预防 文件控制 安全智能过滤 有关详细信息，请参阅IPS 许可证，第 7 页
恶意软件 防御	订用	恶意软件 防御 Secure Secure Malware Analytics 文件存储 （IPS 许可证是恶意软件 防御 许可证的前提条件。） 有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的恶意软件防御许可证，第 7 页和文件和恶意软件策略的许可证要求。
运营商	Firepower 4100/9300、Cisco Secure Firewall 3100/4200 和 Firewall Threat Defense Virtual 的订用	Diameter、GTP/GPRS、M3UA 和 SCTP 检测 有关详细信息，请参阅运营商许可证，第 8 页。
URL 过滤	订用	基于类别和信誉的 URL 过滤 有关详细信息，请参阅URL 过滤许可证，第 9 页。 （IPS 许可证是 URL 过滤 许可证的前提条件。）
Firewall Management Center Virtual	• 定期智能许可-永久 • 特定许可证预留- 订用	平台许可证决定 Firewall Management Center Virtual 可以管理的设备数量。 有关详细信息，请参阅Firewall Management Center Virtual许可证，第 6 页。
出口管制功能	永久	受国家安全、外交政策和反恐怖主义法律和法规约束的功能；请参阅出口控制功能的许可，第 10 页。

您分配的许可证	持续时间	授予的功能
远程访问 VPN： • Secure Client Premier • Secure Client Advantage • 仅限 Secure Client VPN	订用或永久	远程访问 VPN 配置。您的帐户必须允许出口控制功能，以便配置远程访问 VPN。在注册设备时，您需要选择是否满足出口要求。 可以使用任何有效 Secure Client 许可证。可用功能不因许可证类型不同而不同。 有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的Secure Client许可证，第 10 页和 *VPN* 许可。

注释 订用许可证是基于期限的许可证。

Firewall Management Center Virtual许可证

Firewall Management Center Virtual 需要一个与其可管理的设备数量相关的平台许可证。

Firewall Management Center Virtual 支持智能许可。

在常规智能许可中，这些许可证是永久的。

在指定许可证预留 (SLR) 中，这些许可证基于订用。

注释 对于 FMCv 上新设备的附加许可证要求，建议迁移到支持其他设备的更高的 Firewall Management Center Virtual 型号。

基础版许可证

基础版 许可证允许您：

- 配置设备以执行交换和路由（包括 DHCP 中继和 NAT）
- 将设备配置为高可用性对
- 配置集群
- 通过将用户和应用条件添加到访问控制规则实施用户和应用控制
- 更新思科漏洞数据库 (VDB) 和地理位置数据库 (GeoDB)。
- 下载入侵规则，例如 SRU/LSP。但是，除非已启用 IPS 许可证，否则无法将具有入侵策略的访问控制策略或规则部署到设备。

Cisco Secure Firewall 3100/4200

您在购买 Cisco Secure Firewall 3100/4200 时获得 基础版 许可证。

其他型号

除使用特定许可证预留的部署外，对于已注册到 防火墙管理中心的每个帐户， 基础版 许可证会自动添加到您的帐户。对于特定许可证预留，您需要将 基础版 许可证添加到您的帐户。

恶意软件防御许可证

通过恶意软件防御许可证，您可以执行恶意软件防护和 Secure Secure Malware Analytics。通过此功能，您可以使用设备检测并阻止通过网络传输的文件中的恶意软件。要支持此功能许可证，您可以购买恶意软件 防御 (AMP) 服务订阅作为独立订阅，或与 IPS (TM) 或 IPS 和 URL 过滤 (TMC) 订用。IPS 许可证是获得恶意软件 防御 许可证的前提条件。

注释 已启用恶意软件防御许可证的托管设备会定期尝试连接到安全恶意软件分析云，即使尚未配置动态分析也如此。因此，设备的接口流量控制面板构件显示传输的流量；这是预期行为。

配置恶意软件防护作为文件策略的一部分，然后与一个或多个访问控制规则相关联。文件策略可以检测到用户通过特定应用协议上传或下载特定类型文件。恶意软件防护 支持使用本地恶意软件分析和文件预分类来检查一组受限的恶意软件文件类型。您也可以将特定文件类型下载并提交到 Secure Secure Malware Analytics 云进行动态和 Spero 分析，从而确定文件是否包含恶意软件。对于这些文件，您可以查看网络文件轨迹，其中详述文件通过网络所采用的路径。恶意软件防御许可证还可用于将特定文件添加至文件列表，并在文件策略中启用文件列表，从而在检测时自动允许或拦截这些文件。

请注意，仅在部署 恶意软件防护 和 Secure Secure Malware Analytics时，才需要恶意软件 防御 许可证。恶意软件 防御 许可证，则 防火墙管理中心 可以从安全恶意软件分析云接收 Cisco Secure Endpoint 恶意软件事件和危害表现 (IOC)。

另请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的文件和恶意软件策略的许可证要求中的重要信息。

禁用此许可证时：

- 系统会停止查询安全恶意软件分析云，并且还会停止确认从安全恶意软件分析云发送的追溯性事件。
- 如果现有访问控制策略包含恶意软件防护 配置，则无法对其重新部署。
- 请注意，在禁用恶意软件 防御 许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗口到期后，系统会向这些文件分配处置情况 `Unavailable`。

如果许可证到期，上述功能的授权将停止，而 防火墙管理中心 将进入不合规状态。

IPS 许可证

IPS 许可证可用于执行入侵检测和阻止、文件控制和安全智能过滤：

- 入侵检测和防御可用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。
- 文件控制 可用于检测和/或阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。 恶意软件防护需要恶意软件 防御 许可证， 可用于基于某组受限文件类型的处置情况对其进行检查和阻止。
- 安全智能过滤 ，允许您在流量接受访问控制规则的分析之前，拒绝发送到特定 IP 地址、URL 和DNS域名或从其发送的流量，即，将其阻止。动态源可用于根据最新智能立即阻止连接。或者，可将“仅监控”设置用于安全智能过滤。

您可以购买 IPS 许可证作为独立订用 (T) 或与 URL 过滤 (TC)、恶意软件 防御 (TM) 或二者的组合 (TMC)。

禁用此许可证时：

- 防火墙管理中心 会停止从受影响设备确认入侵和文件事件。因此，使用这些事件作为触发器条件的关联规则停止开启。
- 防火墙管理中心 将不会连接互联网获取思科提供的信息或第三方安全智能信息。
- 在重新启用 IPS 之前，您无法重新部署现有入侵策略。

如果许可证到期，上述功能的授权将停止，而 防火墙管理中心 将进入不合规状态。

运营商许可证

运营商许可证，可以实现以下门户检查功能：

- Diameter - Diameter是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。
- GTP/GPRS—GPRS 隧道协议 (GTP) 用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。
- M3UA—MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接信令系统 7 (SS7) 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。
- SCTP - 流控制传输协议 (SCTP) 是支持基于 IP 网络的 SS7 协议的传输层协议。它支持 4G LTE 移动网络架构。SCTP 可以处理多个同步数据流、多路复用数据流，并提供更多安全功能。

注释 在设备上启用此许可证后，请使用 FlexConfig 策略启用协议检测。

运营商许可证 PID 按系列提供，而不按设备型号提供。您可以在评估模式下或使用智能许可证为每台设备启用此许可证。

Firepower 4100/9300、Cisco Secure Firewall 3100/4200 和 Firewall Threat Defense Virtual 的运营商许可证是基于期限的。此许可证还支持特定许可证预留。

支持的设备

支持运营商许可证的设备包括：

- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140
- Firepower 4112
- Firepower 4115
- Firepower 4125
- Firepower 4145
- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245
- Firepower 9300
- Firewall Threat Defense Virtual

URL 过滤许可证

URL 过滤许可证可用于编写访问控制规则，该规则可根据受监控主机请求的 URL 确定可横越网络且与那些 URL 的相关信息关联的流量。要支持此功能许可证，您可以购买 URL 过滤 服务订阅作为独立订阅，或与 IPS (TC) 或威胁和恶意软件防御 (TMC) 订用一道购买。IPS 许可证是获得该许可证的前提条件。

提示 如果没有 URL 过滤许可证，则可以指定要允许或阻止的单个 URL 或 URL 组。这个选项将对网络流量进行精细和自定义控制，但是，不允许使用 URL 类别和信誉数据来过滤网络流量。

虽然您无需 URL 过滤许可证即可将基于类别和信誉的 URL 条件添加到访问控制规则，但 防火墙管理中心 将不会下载 URL 信息。只有先将 URL 过滤许可证添加到 防火墙管理中心，然后在该策略针对的设备上进行启用，才能部署访问控制策略。

禁用此许可证时：

- 您可能会失去对根据URL类别和信誉ACP规则过滤网络流量的访问权限。将继续支持手动URL过滤选项。

- 具有 URL 条件的访问控制规则会立即停止过滤 URL。
- 您的 防火墙管理中心 不再可供下载 URL 数据更新。
- 如果现有访问控制策略包括的规则带有基于类别和信誉的URL条件，则不能重新部署现有的访问控制策略。

如果许可证到期，上述功能的授权将停止，而 防火墙管理中心 将进入不合规状态。

Secure Client许可证

您可以使用 Secure Client 和基于标准的 IPSec / IKEv2 配置远程访问 VPN。

要启用远程访问 VPN 功能，必须购买并启用以下许可证之一： Secure Client Advantage、 Secure Client Premier 或 仅限 Secure Client VPN。如果你有 Secure Client Advantage 和 Secure Client Premier ，并想同时使用这两个许可证，则可以两个都选择。 仅限 Secure Client VPN许可证不能与 **Apex** 或 **Plus**一起使用。 Secure Client 许可证必须与智能帐户共享。有关更多说明，请参阅http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

如果指定的设备不具有至少其中一个指定的Secure Client许可证类型的权利，则无法将远程访问 VPN 配置部署到设备。如果注册的许可证不符合规定或权利到期，系统将显示授权警报和运行状况事件。

使用远程访问 VPN 时，您的智能帐户必须已启用导出控制功能（强加密）。需要强加密（高于 DES），才能与 Secure Client 客户端成功建立远程访问 VPN 连接。

如果以下情况属实，则无法部署远程访问 VPN：

- 防火墙管理中心上的智能许可在评估模式下运行。
- 您的智能帐户未配置为使用导出控制功能（强加密）。

出口控制功能的许可

需要出口控制功能的功能

某些软件功能受国家安全、外交政策和反恐怖主义法律和法规约束。这些出口控制功能包括：

- 安全认证合规性
- 远程访问 VPN
- 具有强加密的站点间 VPN
- 具有强加密的 SSH 平台策略
- 具有强加密的 SSL 策略
- 具有强加密的功能，例如 SNMPv3

如何确定系统当前是否启用了出口控制功能

要确定系统当前是否启用了出口控制功能：转到 **系统** (⚙) > **许可证** > **智能许可证**，查看**导出控制功能**是否显示为**已启用**。

关于启用出口控制功能

如果 **出口控制功能** 显示 **禁用**，而您想要使用需要强加密的功能，有两种方式。您的组织可能有资格使用其中一种方法（或者二者皆不可使用），但不可同时使用这两种方法。

- 在智能软件管理器中生成新的产品实例注册令牌时，如果 没有 启用出口控制功能的选项：

  Cisco批准后，您可以向帐户手动添加强加密许可证，以便使用导出控制功能。有关详细信息，请参阅对于无全局权限的帐户启用出口控制功能，第 29 页

- 如果在智能软件管理器中生成新的产品实例注册令牌时，显示选项“在使用此令牌注册的产品上允许导出控制功能”，请确保在生成令牌之前选中该选项。

  如果未为用于注册 防火墙管理中心的产品实例注册令牌启用导出控制功能，则必须使用启用了导出控制功能的新产品实例注册令牌取消注册，然后重新注册 防火墙管理中心 。

如果在评估模式下或在上 防火墙管理中心 启用强加密之前将设备注册到 防火墙管理中心，请重新启动每台托管设备以提供强加密。在高可用性部署中，主用和备用设备必须同时重启以避免出现主主状态。

授权永久有效，无需订用。

更多信息

有关出口控制的一般信息，请参阅https://www.cisco.com/c/en/us/about/legal/global-export-trade.html。

Firewall Threat Defense Virtual许可证

本部分描述可用于 Firewall Threat Defense Virtual 的性能分级许可授权。

可以在任何受支持的Firewall Threat Defense Virtual vCPU/内存配置中使用任何 Firewall Threat Defense Virtual 许可证。这可让 Firewall Threat Defense Virtual 客户在各种各样的 VM 资源占用空间中运行。这还会增加受支持的 AWS 和 Azure 实例类型的数量。配置 Firewall Threat Defense Virtual VM 时，支持的 vCPU 最大核数为 16（对于 VMware 和 KVM 上的 FTDv；支持的最大内存为 32GB RAM 。

Firewall Threat Defense Virtual 智能许可的性能级别

RA VPN 的会话限制由安装的 Firewall Threat Defense Virtual 平台授权级别确定，并通过速率限制器强制执行。下表总结了基于授权层和速率限制器的会话限制。

表 *3:* 基于授权的 *Firewall Threat Defense Virtual* 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000
FTDvU	32 核/64 GB	不受限制	20,000
FTDvU	64 核/128 GB	不受限制	32,000

FTDv 性能级许可准则和限制

许可 Firewall Threat Defense Virtual 设备时，请时刻注意以下准则和限制。

- Firewall Threat Defense Virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。
- 可以在任何受支持的 Firewall Threat Defense Virtual 核心/内存配置中使用任何 Firewall Threat Defense Virtual 许可证。这可让 Firewall Threat Defense Virtual 客户在各种各样的 VM 资源占用空间中运行。
- 无论您的设备是处于评估模式还是已注册到 思科智能软件管理器，您都可以在部署 Firewall Threat Defense Virtual时选择性能级别。

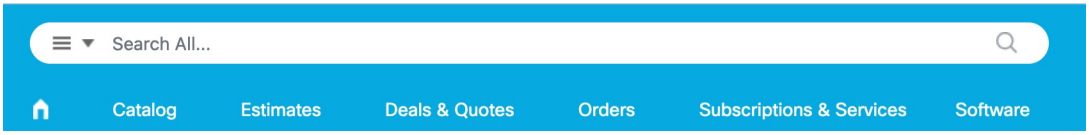
注释 确保智能许可帐户包含所需的可用许可证。选择与您帐户中的许可证相匹配的级别很重要。如果要将 Firewall Threat Defense Virtual 升级到 7.0 版，可以选择 **FTDv - 变量 (FTDv - Variable)** 来保持当前的许可证合规性。Firewall Threat Defense Virtual 会根据您的设备功能（内核数/RAM）继续执行会话限制。

- 部署新 Firewall Threat Defense Virtual 设备或使用 REST API 调配 Firewall Threat Defense Virtual 时，默认性能级别为 FTDv50。
- 基础版许可证以订用为基础，并映射到性能级别。您的虚拟帐户需要具有 Firewall Threat Defense Virtual 设备的 基础版 许可证授权，以及 IPS 、恶意软件防御和 URL 过滤 许可证的授权。
- 每个 HA 对等体使用一个授权，并且每个 HA 对等体上的授权必须匹配，包括基础版许可证。
- 高可用性对的性能级别更改应应用于主对等体。
- 您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。
- 通用 PLR 许可单独应用于高可用性对中的每台设备。辅助设备不会自动镜像主设备的性能级别，而是必须手动更新。

许可证 PID

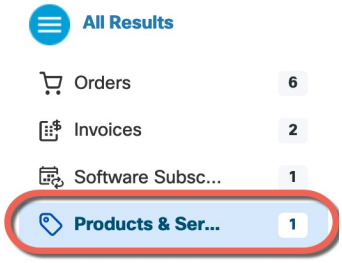
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的**搜索全部 (Search All)** 字段。

图 *1:* 许可证搜索



从结果中选择**产品和服务 (Products & Services)**。

图 *2:* 结果



Firewall Management Center Virtual PID

- VMware：
  - SF-FMC-VMW-2-K9 - 2 设备
  - SF-FMC-VMW-10-K9 - 10 设备
  - SF-FMC-VMW-K9 - 25 设备
  - SF-FMC-VMW-300-K9 - 300 设备
- KVM：
  - SF-FMC-KVM-2-K9 - 2 设备
  - SF-FMC-KVM-10-K9 - 10 设备
  - SF-FMC-KVM-K9 - 25 设备
- 基于 PAK 的 VMware：
  - FS-VMW-2-SW-K9 - 2 设备
  - FS-VMW-10-SW-K9 - 10 设备
  - FS-VMW-SW-K9 - 25 设备

Firewall Threat Defense Virtual PID

订购 FTDV-SEC-SUB 时，必须选择 基础版 许可证和可选功能许可证（12 个月期限）：

- 基础版许可证：
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS 、恶意软件 防御和 URL 许可证组合：
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- 运营商 — FTDV_CARRIER
- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Firepower 1010 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR1010T-TMC=

  当您将上述 PID 添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Firepower 1100 PID

- IPS 、恶意软件 防御和 URL 许可证组合：

- L-FPR1120T-TMC=
- L-FPR1140T-TMC=
- L-FPR1150T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR1120T-TMC-1Y
- L-FPR1120T-TMC-3Y
- L-FPR1120T-TMC-5Y
- L-FPR1140T-TMC-1Y
- L-FPR1140T-TMC-3Y
- L-FPR1140T-TMC-5Y
- L-FPR1150T-TMC-1Y
- L-FPR1150T-TMC-3Y
- L-FPR1150T-TMC-5Y

- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Cisco Secure Firewall 1210/1220 PIDs

- 基础版许可证：
  - 自动包含
- IPS 、恶意软件防御和 URL 许可证组合：
  - L-CSF1210CET-TMC=
  - L-CSF1210CPT-TMC=
  - L-CSF1220CXT-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-CSF1210CE-TMC-1Y
- L-CSF1210CE-TMC-3Y
- L-CSF1210CE-TMC-5Y
- L-CSF1210CP-TMC-1Y
- L-CSF1210CP-TMC-3Y
- L-CSF1210CP-TMC-5Y

- L-CSF1220CX-TMC-1Y
- L-CSF1220CX-TMC-3Y
- L-CSF1220CX-TMC-5Y

- 强加密 (3DES/AES)：
  - L-CSF1200TD-ENCK9=。仅当帐户未获授权使用强加密时需要。
- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Cisco Secure Firewall 1230/1240/1250 PID

- 基础版许可证：
  - 自动包含
- IPS 、恶意软件防御和 URL 许可证组合：
  - L-CSF1230T-TMC=
  - L-CSF1240T-TMC=
  - L-CSF1250T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-CSF1230-TMC-1Y
  - L-CSF1230-TMC-3Y
  - L-CSF1230-TMC-5Y
  - L-CSF1240-TMC-1Y
  - L-CSF1240-TMC-3Y
  - L-CSF1240-TMC-5Y
  - L-CSF1250-TMC-1Y
  - L-CSF1250-TMC-3Y
  - L-CSF1250-TMC-5Y
- 强加密 (3DES/AES)：
  - L-CSF1200TD-ENCK9=。仅当帐户未获授权使用强加密时需要。
- Cisco Secure Client — 请参阅 Cisco Secure Client 订购指南。

Cisco Secure Firewall 3100 PID

- 基础版许可证：
  - 自动包含
- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR3110T-TMC =
  - L-FPR3120T-TMC =
  - L-FPR3130T-TMC =
  - L-FPR3140T-TMC =

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR3105T-TMC-1Y
  - L-FPR3105T-TMC-3Y
  - L-FPR3105T-TMC-5Y
  - L-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y
  - L-FPR3120T-TMC-5Y
  - L-FPR3130T-TMC-1Y
  - L-FPR3130T-TMC-3Y
  - L-FPR3130T-TMC-5Y
  - L-FPR3140T-TMC-1Y
  - L-FPR3140T-TMC-3Y
  - L-FPR3140T-TMC-5Y
- 运营商 - L-FPR3K-FTD-CAR=
- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Firepower 4100 PID

- IPS 、恶意软件 防御和 URL 许可证组合：

- L-FPR4112T-TMC=
- L-FPR4115T-TMC=
- L-FPR4125T-TMC=
- L-FPR4145T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4112T-TMC-1Y
- L-FPR4112T-TMC-3Y
- L-FPR4112T-TMC-5Y
- L-FPR4115T-TMC-1Y
- L-FPR4115T-TMC-3Y
- L-FPR4115T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y

- 运营商 - L-FPR4K-FTD-CAR=
- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Cisco Secure Firewall 4200 PID

- 基础版许可证：
  - 自动包含
- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4215T-TMC-1Y

- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y
- L-FPR4245T-TMC-5Y

- 运营商 - L-FPR4200K-FTD-CAR=
- Cisco Secure Client-请参阅 Cisco Secure Client 订购指南。

Firepower 9300 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y
- 运营商 - L-FPR9K-FTD-CAR=
- Cisco Secure Client-请参阅 Cisco AnyConnect 订购指南。

ISA 3000 PID

- IPS 、恶意软件 防御和 URL 许可证组合：
  - L-ISA3000T-TMC=

  当您将上述 PID 添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-ISA3000T-TMC-1Y
  - L-ISA3000T-TMC-3Y
  - L-ISA3000T-TMC-5Y
- Cisco Secure Client-请参阅 Cisco AnyConnect 订购指南。

许可的要求和前提条件

对于特定许可证预留的要求，请参阅 特定许可证预留的要求和前提条件 ， 第 37 页。

一般前提条件

- 确保在 防火墙管理中心 和托管设备上配置了 NTP。时间必须同步才能成功注册。

  对于 Firepower 4100/9300，必须使用与 防火墙管理中心相同的机箱 NTP 服务器在机箱上配置 NTP。

支持的域

全局，除非另有说明。

用户角色

- 管理员

高可用性、集群和多实例许可的要求和前提条件

本节介绍 高可用性（ 设备高可用性 和 Firewall Management Center Virtual 高可用性）、集群和多实例部署的许可要求。

防火墙管理中心 高可用性许可

每台设备都需要相同的许可证，无论是由单个 防火墙管理中心 管理还是由 防火墙管理中心高可用性对（硬件或虚拟）中的管理。

示例： 如果要对由 防火墙管理中心 对管理的两个设备启用高级恶意软件保护，请购买两个 恶意软件防御 许可证和两个 TM 订用，向智能软件管理器注册主要 防火墙管理中心 ，然后将许可证分配给主要 防火墙管理中心上的两个设备。

只有主用 防火墙管理中心 会向智能软件管理器注册。故障转移发生时，系统与智能软件管理器通信，以释放原始主用 防火墙管理中心 中的许可证授权，并将其分配到新的主用 防火墙管理中心。

在特定许可证预留部署中，只有主 防火墙管理中心 需要特定许可证预留。

硬件 防火墙管理中心

高可用性对中的 防火墙管理中心硬件不需要特殊许可证。

Firewall Management Center Virtual

您将需要两个相同许可的 Firewall Management Center Virtual。

示例： 对于管理 10 台设备的 Firewall Management Center Virtual 高可用性对，您可以使用：

- 两（2） Firewall Management Center Virtual 10个授权
- 10 个设备许可证

如果中断高可用性对，则会释放与辅助 Firewall Management Center Virtual 关联的 Firewall Management Center Virtual 授权。（在本例中，您将有两个独立的 Firewall Management Center Virtual 10。）

设备高可用性许可

高可用性配置中的两台 设备必须具有相同的许可证。

高可用性配置需要两种许可证权利；对中的每个设备各一个。

在建立高可用性之前，将哪些许可证分配给辅助/备用设备并不重要。进行高可用性配置期间，防火墙管理中心 会释放分配给备用设备的所有不必要的许可证，并用分配给主/主用设备的相同许可证替换它们。例如，如果主用设备具有 基础版 许可证和 IPS 许可证，而备用设备只有 基础版 许可证，防火墙管理中心 将与智能软件管理器通信，以从您的备用设备的账户获取可用 IPS 许可证。如果您的许可证帐户不包含足够的购买权利，则您的帐户将在您购买正确数量的许可证之前变得不符合要求。

设备集群许可

每个 Firewall Threat Defense Virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 防火墙管理中心时，您可以指定要用于该集群的功能许可证。在创建集群之前，将哪些许可证分配给数据节点并不重要；控制节点的许可证设置将复制到每个数据节点。可以通过在**系统** (⚙) > **许可证** > **智能许可证**中点击**编辑许可证**，或选择**设备** > **设备管理**，点击集群的**编辑** (✎)，然后在**集群** > **许可证**区域中点击**编辑** (✎)来修改集群的许可证。

注释 如果在 防火墙管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 防火墙管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

许可多实例部署

所有许可证按每个引擎/机箱（对于 Firepower 4100）或每个安全模块（对于 Firepower 9300）予以使用，而不是按每个容器实例使用。请查看以下详细信息：

- 基础版 许可证自动分配：每个 安全模块/引擎一个。
- 功能许可证手动分配到每个实例；但每个 安全模块/引擎每个功能只能使用一个许可证。例如，对于具有 3 个安全模块的 Firepower 9300，每个模块只需要一个 URL 过滤 许可证，总共需要 3 个许可证，而无须考虑正在使用的实例数。

例如：

表 *4: Firepower 9300* 上容器实例的许可证使用情况示例

Firepower 9300	实例	许可证
安全模块 1	实例 1	基础版、 URL 过滤、 恶意软件防御
	实例 2	基础版、 URL 过滤
	实例 3	基础版、 URL 过滤
安全模块 2	实例 4	基础版、 IPS
	实例 5	基础版、 URL 过滤、 恶意软件防御、 IPS
安全模块 3	实例 6	基础版、 恶意软件防御、 IPS
	实例 7	基础版、 IPS

表 *5:* 许可证总数

基础版	**URL** 过滤	恶意软件防御	**IPS**
3	2	3	2

创建思科帐户

您必须拥有思科账户才能申请智能账户并许可任何思科产品。

过程

步骤 1 打开 URL https://id.cisco.com/signin/register 以创建新账户。

步骤 2 输入所有必填字段以创建账户。

下图显示了一个示例。

步骤 3 点击**注册 (Register)**。

系统会向您发送一封包含激活码的邮件，以验证您的邮箱地址。

注释
如果您尚未收到邮件，请通过 web-help@cisco.com 向注册支持团队发送邮件。

步骤 4 在**使用您的邮箱验证 (Verify with your email)** 页面中，输入激活码以完成注册过程，然后点击**验证 (Verify)**。

注册成功后，您将被重定向到登录页面。

下一步做什么

在登录页面输入新创建的账户详细信息，以请求智能账户。请参阅创建智能账户并添加许可证，第 23 页。

创建智能账户并添加许可证

购买许可证之前，您应设置此账户。

开始之前

您的客户代表可以代表您设置智能帐户。如果是这样，则无须按照本程序进行操作，而是从该客户代表处获取访问该帐户所需的信息，并确认可以访问该帐户。

如果您还没有思科账户，则必须创建一个新账户。有关说明，请参阅创建思科账户。

有关智能账户的一般信息，请参阅http://www.cisco.com/go/smartaccounts。

过程

步骤 1 转到创建智能账户 (Create a Smart Account) 页面。系统将提示您使用思科账户登录。

在**创建智能账户 (Create a Smart Account)** 页面中，将显示您的基本账户信息。

步骤 2 点击右上角显示的**我的账户 (My Account)** 图标，然后点击**管理配置文件 (Manage Profile)**。

步骤 3 点击**个人 (Personal)**。

步骤 4 在**您的公司详细信息 (Your Company Details)** 部分中，点击**编辑 (Edit)**。

步骤 5 在**公司或组织 (Company or organization)** 字段中，键入您的组织名称。

步骤 6 如果您的公司信息已存在于我们的数据库中，它将显示在列表中。您可以选择您的公司。

在**地址 (Address)** 下拉列表中，选择您公司的地址。

步骤 7 如果您的公司未在我们的数据库中列出，您可以继续在**公司或组织 (Company or organization)** 字段中输入您的公司信息。

a) 在**地址 (Address)** 下拉列表中，点击下拉箭头，然后点击**添加新地址 (Add New Address)**。

b) 您可以选择以下**地址类型 (Address Type)** 选项之一：

- **公司/组织 (Company/Organization)**：提供您的组织的地址。思科会验证此地址。如果地址和公司名称无法通过国家/地区验证，您可能无法继续。因此，您必须确保提供正确的地址。
- **个人 (Personal)**：提供您的个人地址。

步骤 8 输入与您的公司相关的所有必填字段，然后点击**更新 (Update)**。

您的公司详细信息 (Your Company Details) 部分将显示您输入的公司详细信息。

如果您的公司详细信息已通过验证，系统将显示成功消息。

步骤 9 点击**更新**。

如果您的公司详细信息已通过验证，系统将显示成功消息。

步骤 10 打开在上一个选项卡中打开的**创建智能账户 (Create a Smart Account)** 页面。如果未反映更改，请刷新页面。

或者，您可以使用 https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation URL 打开此页面，然后使用您的凭证登录。

步骤 11 点击**创建帐户 (Create Account)**。

“账户摘要”(Account Summary) 页面将显示您的账户详细信息。

步骤 12 点击**完成 (Done)**。

步骤 13 等待智能帐户已做好设置准备的通知邮件。在收到邮件时，按照指示点击邮件中的链接。

步骤 14 请确保智能许可帐户包含所需的可用许可证。

有关许可证 PID，请参阅 许可证 PID，第 13 页。

下一步做什么

要使用智能软件管理器配置智能许可证，请参阅配置智能许可，第 25 页。

配置智能许可

本节介绍如何通过智能软件管理器或本地智能软件管理器使用智能许可。要使用指定许可证预留，请参阅 配置特定许可证预留 (SLR)，第 36 页。

注册防火墙管理中心以进行智能许可

您可以通过互联网将防火墙管理中心直接注册到智能软件管理器，或者在使用气隙网络时，使用本地智能软件管理器注册。

将防火墙管理中心注册到智能软件管理器

将防火墙管理中心注册到智能软件管理器。

开始之前

- 请确保智能许可帐户包含所需的可用许可证。

  当您从 Cisco 或经销商那里购买设备时，您的许可证应该已链接到您的智能帐户。但是，如果您需要自己添加许可证，请参阅 Cisco 商务工作空间。有关许可证 PID，请参阅 许可证 PID，第 13 页。

- 确保 防火墙管理中心 可以在 smartreceiver.cisco.com 上到达智能软件管理器。
- 确保配置 NTP。在注册过程中，密钥交换发生在智能代理和智能软件管理器之间，因此时间必须同步才能正确注册。

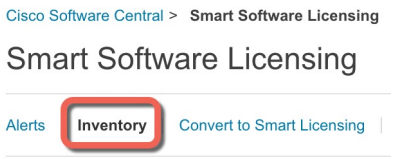
  对于 Firepower 4100/9300，必须使用与 防火墙管理中心相同的机箱 NTP 服务器在机箱上配置 NTP。

- 如果您的阻止有多个 防火墙管理中心，请确保每个 防火墙管理中心 拥有唯一的名称，以与可能注册到同一虚拟账户的其他 防火墙管理中心 进行区分。此名称对于管理智能许可证授权至关重要，而使用模糊名称稍后会出现问题。

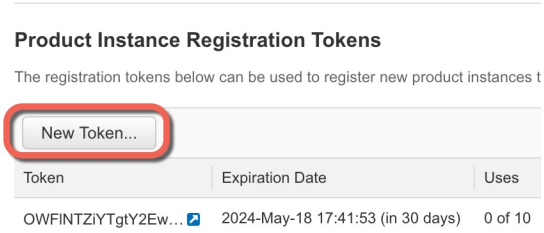
过程

步骤 1 在 智能软件管理器 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

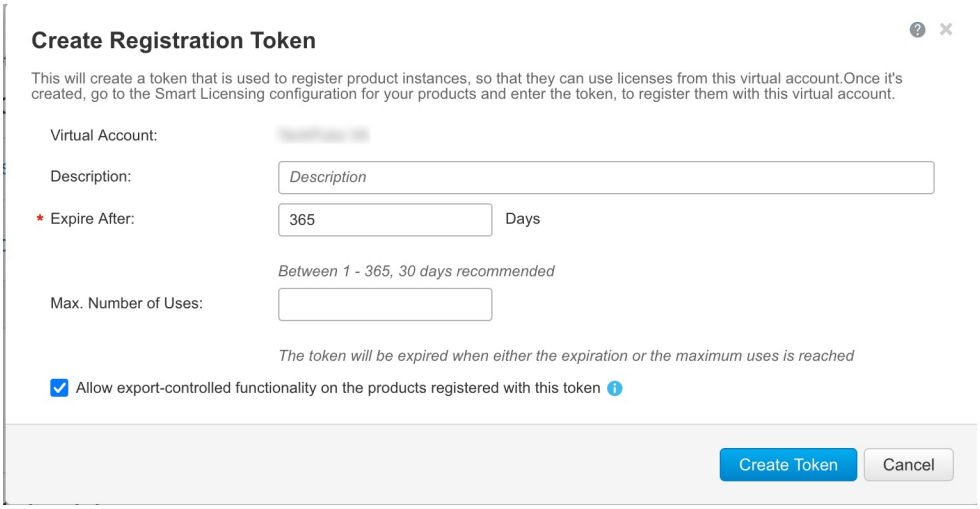
a) 点击**清单 (Inventory)**。



b) 在 **General** 选项卡上，点击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- 说明
- **Expire After** - 思科建议该时间为 30 天。
- 最大使用次数
- 在使用此令牌注册的产品上允许导出控制的功能 **(Allow export-controlled functionaility on the products registered with this token** — 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。如果打算使用此功能，则须立即选择该选项。如果稍后启用此功能，则需要使用新产品密钥重新注册设备并重新加载设备。如果您没有看到此选项，则您的帐户不支持出口控制功能。

系统将令牌添加到您的清单中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册时，请准备好此令牌，以在该程序后面的部分使用。

图 *3:* 查看令牌

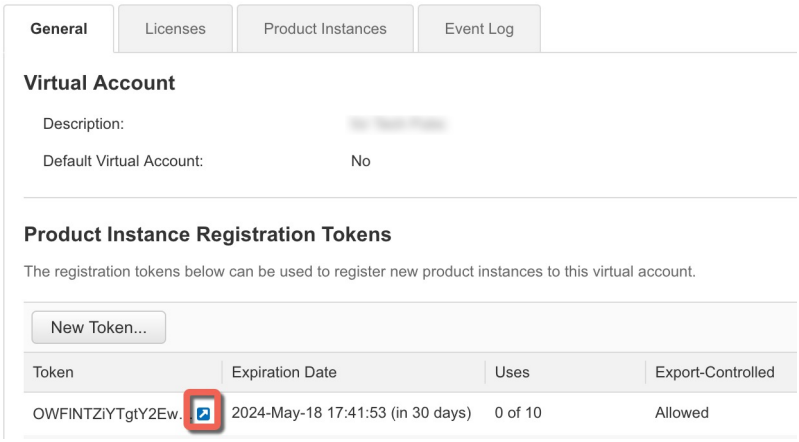
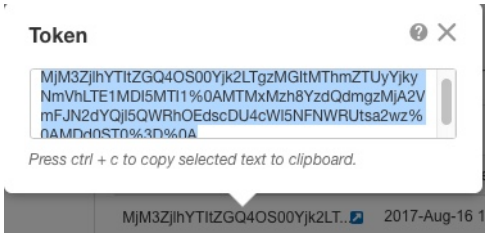


图 *4:* 复制令牌



步骤 2 在 防火墙管理中心上，选择 **系统 (⚙) > 许可证 > 智能许可证**。

步骤 3 点击**注册 (Register)**。

步骤 4 将您从 智能软件管理器 生成的令牌粘贴到 **产品实例注册令牌** 字段中。

确保文本开头和结尾处没有空格或空行。

步骤 5 如果管理中心实例已向智能许可注册，您可以选中 **覆盖现有注册管理中心实例** 复选框以覆盖智能许可中的现有注册管理中心实例。

步骤 6 决定是否向思科发送使用数据。

- Cisco Success Network 功能允许思科收集客户使用指标和统计数据，以分析产品使用情况并提升客户对思科产品的体验。默认情况下启用此功能。要退出向 Cisco 发送 Cisco Success Network 遥测数据，请参阅配置 防火墙管理中心 以与思科共享使用情况指标和统计信息。有关思科收集的遥测数据的更多信息，请点击**示例数据**。
- 借助思科支持诊断功能，思科可以从您的设备收集重要信息，为您提供更好的支持体验。默认情况下启用此功能。要选择不向思科发送思科支持诊断指标，请参阅配置防火墙管理中心 以与思科共享设备运行状况数据。

  注释
  - 启用思科支持诊断后，它会在下一个同步周期应用于设备。 防火墙管理中心 与设备的同步每 30 分钟运行一次。
  - 启用思科支持诊断后，它将自动应用于在此 防火墙管理中心 中注册的任何新设备。

步骤 7 点击 **Apply Changes**（应用更改）。

下一步做什么

- 将设备添加到 防火墙管理中心；请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的将设备添加到 防火墙管理中心。
- 将许可证分配到您的设备；请参阅 将许可证分配给多个托管设备，第 31 页。

将防火墙管理中心注册到本地智能软件管理器

如与智能软件管理器的定期通信，第 2 页中所述，防火墙管理中心必须与 Cisco 定期通信，以维护许可证授权。如果出现以下情况之一，您便可能希望将智能软件管理器本地版（之前称为智能软件卫星服务器）用作代理服务器，以供连接到智能软件管理器：

- 防火墙管理中心为离线状态、连接受限或无连接（即部署于气隙网络中）。

  （有关气隙网络的替代解决方案，请参阅气隙部署的许可选项，第 2 页。）

- 防火墙管理中心具备永久连接，但您希望通过网络中的单个连接管理智能许可证。

智能软件管理器本地版允许您安排同步或手动将智能许可证授权与智能软件管理器同步。

有关 智能软件管理器本地版 的详细信息，请参阅https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem。

过程

步骤 1 部署和设置。智能软件管理器本地版

- 请参阅智能软件管理器本地版的文档，可从https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem获取。
- 在您的智能软件管理器本地版记下 TLS/SSL 证书的 CN。
- 转至 http://www.cisco.com/security/pki/certs/clrca.cer，并将完整的 TLS/SSL 证书正文 （从“-----BEGIN CERTIFICATE-----”到“-----END CERTIFICATE-----”）复制到您在配置期间可访问的某个位置。

步骤 2 将 防火墙管理中心注册到 智能软件管理器本地版。

a) 选择**集成** > **其他集成**。
b) 点击**智能软件管理器本地版**。
c) 选择**连接到思科智能软件管理器本地服务器**。
d) 使用您在此过程的前提条件中收集的CN值，按以下格式输入智能软件管理器本地版的**URL**：

`https://FQDN_or_hostname_of_your_SSM_On-Prem/SmartTransport`

FQDN 或主机名必须与您智能软件管理器本地版提供的证书的 CN 值匹配。

e) 添加新 **SSL 证书**，并粘贴您之前复制的证书文本。
f) 点击 **Apply**。
g) 选择 **系统** (⚙) > **许可证** > **智能许可证** 并点击**注册**。
h) 创建新的智能软件管理器本地版令牌。
i) 复制该令牌。
j) 将该令牌粘贴到管理中心页面上的表中。
k) 点击 **Apply Changes**（**应用更改**）。

管理中心现已注册到智能软件管理器本地版。

步骤 3 将许可证分配给设备后，同步智能软件管理器本地版到智能软件管理器。

请参阅上面的智能软件管理器本地版文档。

步骤 4 安排日常同步次数。

对于无全局权限的帐户启用出口控制功能

如果您的智能帐户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的帐户。

开始之前

- 确保部署尚**不**支持出口控制功能。

  如果您的部署支持出口管制功能，您将看到一个选项，您可以启用在**创建注册令牌**页中智能软件管理器出口控制功能。有关详细信息，请参阅https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html。

- 确保部署未在使用评估许可证。
- 在智能软件管理器 (Smart Software Manager) 中，转至 **清单 (Inventory)** > **许可证 (Licenses)**页面，确认拥有与 防火墙管理中心对应的许可证：

出口控制许可证	防火墙管理中心 型号
思科虚拟 FMC 系列强加密 (3DES/AES)	所有 Firewall Management Center Virtual
思科 FMC 1K 系列强加密 (3DES/AES)	_ _
思科 FMC 2K 系列强加密 (3DES/AES)	__
思科 FMC 4K 系列强加密 (3DES/AES)	__

过程

步骤 1 选择**系统** (⚙) > **许可证** > **智能许可证**。

注释
如果显示 **请求导出密钥**，则表示帐户获准使用出口控制功能，您可继续使用所需功能。

步骤 2 点击**请求导出密钥**以生成导出密钥。

提示
如果出口控制密钥请求失败，则请确保虚拟帐户具备有效的出口控制许可证。

通过点击 **恢复导出密钥**来禁用该出口控制许可证。

下一步做什么

您现在即可部署使用出口控制功能的配置或策略。

记住 在 设备重启之前，由此功能启用的新出口控制许可证和所有功能将不会在这些设备上生效。在此之前，只有受以往许可证支持的功能有效。

在高可用性部署中，需要同时启动 设备以避免出现主主状态。

将许可证分配到设备

将设备注册到 防火墙管理中心时，可以分配大多数许可证。您还可以为每台设备或为多台设备分配许可证。

将许可证分配给单个设备

尽管有一些例外，但如果在托管设备上禁用许可证，就无法使用与该许可证关联的功能。

注释 对于同一 安全模块/引擎上的容器实例，您将对每个实例应用许可证；请注意，对于 安全模块/引擎上的所有实例，安全模块/引擎仅对每个功能占用一个许可证。

注释 对于 集群，您将对整个集群应用许可证；请注意，集群中的每个设备将对每个功能占用单独的许可证。

开始之前

您必须具有管理员或网络管理员权限才能执行此任务。使用多个域时，必须在分叶域中执行此任务。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 在要分配或禁用许可证的设备旁边，点击 **编辑** (✎)。

步骤 3 点击**设备 (Device)**。

步骤 4 点击 **许可证** 部分旁边的 **编辑** (✎)。

步骤 5 选中或清除相应的复选框，以便为设备分配或禁用许可证。

步骤 6 点击**保存**。

步骤 7 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

下一步做什么

验证许可证状态：转至 **系统** (⚙) > **许可证** > **智能许可证**，将设备的主机名或 IP 地址输入“智能许可证”表顶部的过滤器中，验证每个许可证类型是否仅对每个设备显示一个带有 **复选标记**（✔） 的绿色圆圈 。如有任何其他图标，则将鼠标悬停在图标上查看详细信息。

将许可证分配给多个托管设备

受 防火墙管理中心 管理的设备通过 防火墙管理中心获取许可证，而非直接通过智能软件管理器获取。

使用本程序在多个设备上启用许可。

注释 对于同一 安全模块/引擎上的容器实例，您将对每个实例应用许可证；请注意，对于 安全模块/引擎上的所有实例，安全模块/引擎仅对每个功能占用一个许可证。

注释 对于 集群，您将对整个集群应用许可证；请注意，集群中的每个设备将对每个功能占用单独的许可证。

过程

步骤 1 选择**系统** (⚙) > **许可证** > **智能许可证**或**特定许可证**。

步骤 2 点击**编辑许可证**。

步骤 3 对于想要添加到设备的每种类型的许可证：

a) 点击该类型许可证的选项卡。
b) 点击左侧列表中的设备。
c) 点击**添加**将该设备移至右侧列表。
d) 为每个设备重复此操作以接收该类型的许可证。

现在无需再担心是否拥有想要添加的所有设备的许可证。

e) 为想要添加的每种类型许可证重复此子程序。
f) 要删除许可证，请点击设备旁边的 **删除** ( ) 。
g) 点击**应用 (Apply)**。

您可以选择集群并将任何许可证分配给集群的所有节点。

下一步做什么

验证许可证是否已正确安装。请按照监控智能许可证 ， 第 34 页中的程序操作。

管理智能许可

本部分介绍如何管理智能软件许可。

取消注册 防火墙管理中心

从智能软件管理器中取消注册您的防火墙管理中心，以将所有许可证授权释放回您的智能帐户，以便可用于其他设备。例如，如果需要停用防火墙管理中心或重新映像，请取消注册。

有关在未注册状态下执行许可证的详细信息，请参阅 已注销状态 ， 第 4 页 。

过程

步骤 1 选择**系统** ( ) > **许可证** > **智能许可证**。

步骤 2 请点击 **取消注册**（ ）。

同步或重新授权 防火墙管理中心

默认情况下，ID 证书每 6 个月自动更新，许可证授权每 30 天更新。如果您访问互联网的时间有限，或者例如在智能软件管理器中进行了任何许可更改，则可能需要为其中任一项手动续约注册。

过程

步骤 1 选择**系统** (⚙) > **许可证** > **智能许可证**。

步骤 2 要更新 ID 证书，请点击 **同步**（🔄）

步骤 3 要更新许可证授权，请点击 **重新授权**。

监控智能许可状态

系统 (⚙) > **许可证** > **智能许可证**页面的**智能许可证状态**部分提供 防火墙管理中心上许可证使用情况的概览，如下所述。

使用授权

可能的状态值包括：

- **不合规**（✔） - 分配到受管设备的所有许可证均合规，并且 防火墙管理中心 与思科许可证颁发机构通信成功。
- **许可证符合规定，但与许可证授权机构的通信失败** - 设备许可证合规，但 防火墙管理中心 无法与思科许可证颁发机构通信。
- **不合规图标或无法与许可证颁发机构通信**- 一个或多个受管设备使用的许可证不合规，或 防火墙管理中心 已有超过 90 天未与思科许可证颁发机构通信。

产品注册

指定 防火墙管理中心 联系智能软件管理器并向其注册的最后日期。

分配的虚拟帐户

指定用于生成产品实例注册令牌和注册 防火墙管理中心的智能帐户下的虚拟帐户。如果此部署未关联智能帐户内的某个特定虚拟帐户，则不会显示此信息。

出口管制功能

如果启用此选项，则可部署受限制的功能。有关详细信息，请参阅出口控制功能的许可，第 10 页。

Cisco Success Network

指定是否为 防火墙管理中心启用了 Cisco Success Network。如果启用此选项，您可以向思科提供使用情况信息和统计数据，这些信息对为您提供技术支持非常重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。有关详细信息，请参阅配置 防火墙管理中心 以与思科共享使用情况指标和统计信息。

监控智能许可证

要查看 防火墙管理中心 及其管理设备的许可证状态，请使用智能许可证页面。

对于部署中每种类型的许可证，该页面都会列出使用的许可证总数、许可证是合规还是不合规、设备类型以及设备部署所在的域和组。您还可以查看防火墙管理中心的智能许可证状态。在同一安全模块/引擎 上的容器实例仅会为每个 安全模块/引擎使用一个许可证。因此，即使 防火墙管理中心 在每个许可证类型下单独列出每个容器实例，功能许可证类型占用的许可证数量也将为一。

除了 **智能许可证** 页面之外，还有其他一些方法可用于查看许可证：

- **产品许可** 控制面板构件提供了许可证概览。

  请参阅将构件添加到控制面板和按用户角色划分的控制面板构件可用性和产品许可构件。

- **设备管理** 页面 （**设备** > **设备管理**）列出应用于每个托管设备的许可证。
- **智能许可证监控** 运行状况模块在运行状况策略中使用时传达许可证状态。

过程

步骤 1 选择**系统** (⚙) > **许可证** > **智能许可证**。

步骤 2 在**智能许可证**表中，点击每个**许可证类型**文件夹左侧的箭头以展开该文件夹。

步骤 3 在每个文件夹中，验证 **许可证状态** 列中每个设备是否有具有 **复选标记**（✔） 的绿色圆圈 。

注释
如果您看到重复的 Firewall Management Center Virtual 许可证，则每个许可证都代表一个托管设备。

如果每个设备都显示带 **复选标记**（✔）的绿色圆圈，则表示设备已正确许可并可供使用。

如果未显示带 **复选标记**（✔）的绿色圆圈，请将鼠标悬停在状态图标上以查看消息。

下一步做什么

- 如果存在不带 **复选标记**（✔）的绿色圆圈的任何设备，则可能需要购买更多许可证。

智能许可疑难解答

我的智能账户中没有显示预期许可证

如果期望看到的许可证未出现在您的智能账户中，则请尝试以下操作：

- 确保许可证不在其他虚拟账户中。您的组织的许可证管理员也许可以给予协助。
- 联系您的许可证销售者，确定许可证已转移到您的账户中。

无法连接到智能许可证服务器

首先检查明显的原因。例如，确保您的 防火墙管理中心 具有外部连接。参阅访问的互联网资源。

意外出现不合规通知或其他错误

- 如果设备已向其他防火墙管理中心注册，则需要先取消注册原始防火墙管理中心，然后才能在新的防火墙管理中心下许可该设备。请参阅取消注册 防火墙管理中心，第 32 页。
- 检查订用许可证的期限是否已到期。

排除其他问题

有关其他常见问题的解决方案，请参阅 https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

转换经典许可证以在 上使用

您可以使用许可证注册门户或智能软件管理器转换许可证，并且可以转换已分配到某个设备的未使用产品授权密钥 (PAK) 或经典许可证。

注释 您无法撤销此过程。即使某个智能许可证原为经典许可证，您也无法将其转换为经典许可证。

在 Cisco.com 上的文档中，经典许可证也称为“传统”许可证。

开始之前

- 当经典许可证仍为尚未分配到产品实例的未使用 PAK 时，将其转换为智能许可证最为简单。
- 您的硬件必须能够运行 。请参阅《*Cisco Secure Firewall Threat Defense* 兼容性指南》，网址：https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html。
- 您必须拥有智能帐户。如果没有，请创建一个。请参阅创建智能账户并添加许可证，第 23 页。
- 智能帐户中必须显示要转换的 PAK 或许可证。
- 如果使用许可证注册门户而非智能软件管理器进行转换，则必须拥有智能账户凭证才能发起转换过程。

过程

步骤 1 您将执行的转换过程取决于许可证是否已被占用：

- 如果要转换的 PAK 从未被使用，请按照说明转换 PAK。
- 如果要转换的 PAK 已分配到某个设备，请按照说明转换经典许可证。

  请确保现有的经典许可证仍向设备注册。

步骤 2 请参阅以下文档中适用于您的转换类型（PAK 或已安装的经典许可证）的说明进行操作：

- 要使用许可证注册门户转换 PAK 或许可证：
  - 在 使用智能账户管理思科经典许可中观看引导您完成转换过程中许可证注册门户部分的视频。
  - 在 https://tools.cisco.com/SWIFT/LicensingUI/Home 上登录到许可证注册门户 (LRP)，然后按照上述文档中的说明进行操作。
- 要使用智能软件管理器转换 PAK 或许可证，请执行以下操作：
  - 《混合许可证转换智能软件许可证快速参考指南》：

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - 在 https://software.cisco.com/#SmartLicensing-LicenseConversion 上登录智能软件管理器，按照上述文档中适用于您的转换类型（PAK 或已安装的经典许可证）的说明进行操作。

步骤 3 在硬件上全新安装 。

请参阅 安装和升级指南 中有关您的硬件的说明。

步骤 4 如果要使用 设备管理器 将此设备作为独立设备进行管理：

有关 设备管理器 配置指南中的设备许可信息，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

跳过此程序的其余步骤。

步骤 5 如果已在 防火墙管理中心上部署智能许可：

a) 在新的 设备上设置智能许可。

请参阅将许可证分配给多个托管设备，第 31 页。

b) 验证新的智能许可证是否已成功应用到该设备。

请参阅监控智能许可证，第 34 页。

步骤 6 如果尚未在 防火墙管理中心上部署智能许可：

请参阅配置智能许可，第 25 页。（请跳过不适用或已完成的任何步骤。）

配置特定许可证预留 (SLR)

您可以使用特定许可证预留功能在气隙网络中部署智能许可。

注释 思科对特定许可证预留使用了各种名称，包括SLR、SPLR、PLR和永久许可证预留。思科也可能使用这些术语来指代类似但不一定相同的许可模式。

特定许可证预留启用时，防火墙管理中心会在指定的持续时间内预留来自虚拟账户的许可证，而无需访问智能软件管理器或使用 智能软件管理器本地版。

需要接入互联网的功能（例如对公共网站的 URL 查找或上下文交叉启动）将无法工作。

思科不会收集使用特定许可证预留的部署的网络分析或遥测数据。

特定许可证预留的要求和前提条件

- 如果当前使用常规智能许可，请在实施特定许可证预留之前注销防火墙管理中心。有关信息，请参阅取消注册 防火墙管理中心，第 32 页。

  当前部署到防火墙管理中心的所有智能许可证将返回账户的可用许可证池中，在实施特定许可证预留时即可重用它们。

- 特定许可证预留需要与标准智能许可相同数量和类型的许可证。
- （推荐）如果在高可用性配置中部署 防火墙管理中心 对，请注意以下事项：
  - 在分配许可证之前配置高可用性。如果您已将许可证分配给辅助 防火墙管理中心上的设备，请务必取消分配。
  - 如果将 SLR 许可证分配给主设备 防火墙管理中心，则当辅助设备 防火墙管理中心 在故障转移后变为主用设备时，您无法将SLR许可证添加到辅助设备 防火墙管理中心。您必须执行以下操作之一：
    - 执行故障转移，使主 防火墙管理中心 处于活动状态。
    - 取消分配并将许可证重新分配给辅助 防火墙管理中心。

验证您的智能帐户是否已准备好部署特定许可证预留

为防止部署特定许可证预留时发生问题，请先完成本程序，再在 防火墙管理中心中进行任何更改。

开始之前

- 确保已满足特定许可证预留的要求和前提条件，第 37 页中的要求。
- 确保拥有智能软件管理器凭证。

过程

步骤 1 登录到智能软件管理器：

https://software.cisco.com/#SmartLicensing-Inventory

步骤 2 如果适用，请从页面右上角选择正确的帐户。

步骤 3 如有必要，请点击**清单 (Inventory)**。

步骤 4 点击 **许可证**。

步骤 5 请验证以下项目：

- 显示**许可证预留**按钮。
- 对于将要部署的设备和功能，有足够的平台和功能许可证可供使用，包括设备的 Firewall Management Center Virtual 授权（如适用）。

步骤 6 如果其中有任何项目缺失或有误，请联系您的客户代表来解决问题。

注释
在解决所有问题之前，请勿继续此过程。

启用特定许可菜单选项

本程序会将 防火墙管理中心中的“智能许可证”菜单选项更改为“特定许可证”。

过程

步骤 1 使用 USB 键盘和 VGA 显示器访问 防火墙管理中心 ，或使用 SSH 访问管理界面。

步骤 2 登录 防火墙管理中心 CLI **管理员** 账户。

步骤 3 输入 **expert** 命令以访问 Linux 外壳。

步骤 4 执行以下命令以访问特定许可证预留选项：

sudo manage_slr.pl

示例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
```

```
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

步骤 5 选择选项 **2**即可启用特定许可证预留。

步骤 6 选择选项 **0** 退出 manage_slr 实用程序。

步骤 7 键入 **exit** 退出 Linux 外壳。

步骤 8 输入 **exit** 退出命令行接口。

步骤 9 验证是否可以在 防火墙管理中心 Web 界面中访问**特定许可证预留**页面：

- 如果当前显示**系统 (⚙) > 许可证 > 智能许可证**页面，请刷新页面。
- 否则，选择 **系统 (⚙) > 许可证 > 特别许可证**。

将特定许可证预留授权码输入 防火墙管理中心

过程

步骤 1 生成预留申请代码。

a) 在 防火墙管理中心上，选择 **系统 (⚙) > 许可证 > 特别许可证**。
b) 点击**生成 (Generate)**。
c) 记下**预留申请代码**。

步骤 2 生成预留授权码。

a) 转至思科智能软件管理器： https://software.cisco.com/#SmartLicensing-Inventory
b) 如有必要，请从页面右上角选择正确的帐户。
c) 如有必要，请点击**清单 (Inventory)**。
d) 点击 **许可证**。
e) 点击**许可证预留 (License Reservation)**。
f) 将从 防火墙管理中心 生成的代码输入**预留申请代码**框中。
g) 点击**下一步 (Next)**。
h) 选择**预留特定许可证**。
i) 向下滚动以显示整个许可证网格。
j) 在**预留数量**下，输入部署所需的每个平台和功能的许可证数量。

注释

- 您必须为每个受管设备明确包含一个 基础版 许可证，对于多实例部署，必须为每个容器明确包含一个基础许可证。

- 如果您使用 Firewall Management Center Virtual，则必须对每个模块（多实例部署）或每个托管设备（所有其他部署）包括一个平台授权。
- 如果使用强加密功能：
  - 如果您的整个智能账户已启用出口控制功能，则无须在此进行任何操作。
  - 如果您所在组织的授权为“每防火墙管理中心 ”，则您必须选择适当的许可证。

    要为 防火墙管理中心选择正确的许可证名称，请参阅 对于无全局权限的帐户启用出口控制功能， 第 29 页中所述的前提条件。

k) 点击**下一步 (Next)**。

l) 点击**生成授权码**。

根据智能软件管理器，许可证现已处于使用状态。

m) 下载授权码，准备将其输入 防火墙管理中心。

步骤 3 在 防火墙管理中心中输入授权码。

a) 在 防火墙管理中心中，点击 **浏览** 以上传包含从智能软件管理器生成的授权码的文本文件。

b) 点击**安装 (Install)**。

c) 验证**特定许可证预留**页面上的**使用授权**是否显示为“已授权”状态。

d)

步骤 4 点击**预留许可证 (Reserved License)** 选项卡以验证在生成**授权码 (Authorization Code)** 时所选择的许可证。

如果没有看到所需的许可证，请添加必要的许可证。有关详细信息，请参阅更新 Firepower 管理中心的特定许可证。

将特定许可证分配给托管设备

使用本程序将许可证一次性地快速分配到多个托管设备。

您还可以使用本程序禁用许可证，或在设备之间移动许可证。如果您禁用设备的许可证，则不能在设备上使用与该许可证相关的功能。

过程

步骤 1 选择**系统 (⚙) > 许可证 > 特别许可证**。

步骤 2 点击**编辑许可证**。

步骤 3 根据需要点击每个选项卡并将许可证分配到设备。

步骤 4 点击**应用 (Apply)**。

步骤 5 点击**已分配许可证**选项卡，验证许可证是否已正确安装在每个设备上。

步骤 6 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

管理特定许可证预留

本节介绍如何管理特定许可证预留。

重要提示！维护特定许可证预留部署

要更新使部署保持有效的威胁数据和软件，请参阅维护气隙部署。

要确保所有功能继续工作而不发生中断，请监控许可证的到期日期（位于**预留的许可证**选项卡）。如果任何许可证到期，且使用计数大于可用计数，则 防火墙管理中心 将处于不合规状态。

更新特定许可证预留

在特定许可证成功部署在 防火墙管理中心之后，即可使用本程序随时添加或删除授权。

如果您需要在许可证到期后续约，请使用此程序。如果您没有所需的许可证，则以下操作会受到限制：

- 设备注册
- 策略部署

过程

步骤 1 在 防火墙管理中心中，获取此 防火墙管理中心的唯一产品实例标识符：

a) 选择**系统** (⚙) > **许可证** > **特别许可证**。

b) 记下**产品实例**的值。

您将在此过程期间多次使用此值。

步骤 2 在智能软件管理器中，确定要升级的 防火墙管理中心 ：

a) 转至智能软件管理器：

https://software.cisco.com/#SmartLicensing-Inventory

b) 如有必要，请点击**清单**。

c) 点击 **产品实例**。

d) 在**类型**列中查找带有 **FP** 字样的产品实例，并在**名称**列中查找通用 SKU（非主机名）。您也可以借助其他表列中的值来确定 防火墙管理中心 是正确的 防火墙管理中心。点击名称。

e) 查看 **UUID** ，看看它是否是您尝试修改的 防火墙管理中心 的 UUID。

如果不是，则必须重复这些步骤，直至找到正确的 防火墙管理中心。

步骤 3 在思科智能软件管理器中找到正确的防火墙管理中心后，即可更新预留许可证并生成新的授权码：

a) 在显示正确 UUID 的页面上，选择 **操作** > **更新预留许可证**。
b) 根据需要更新预留许可证。

注释

- 您必须为每个受管设备明确包含一个 基础版 许可证，对于多实例部署，必须为每个容器明确包含一个基础许可证。
- 如果您使用 Firewall Management Center Virtual，则必须对每个模块（多实例部署）或每个托管设备（所有其他部署）包括一个平台授权。
- 如果使用强加密功能：
  - 如果您的整个智能账户已启用出口控制功能，则无须在此进行任何操作。
  - 如果您所在组织的授权为“每防火墙管理中心 ”，则您必须选择适当的许可证。

    要为 防火墙管理中心选择正确的许可证名称，请参阅 对于无全局权限的帐户启用出口控制功能，第 29 页中所述的前提条件。

c) 点击**下一步**并验证详细信息。
d) 点击**生成授权码**。
e) 下载授权码，准备将其输入 防火墙管理中心。
f) 保持 **更新预留** 页面处于打开状态。稍后您将在本程序中返回此页面。

步骤 4 更新 防火墙管理中心中的特定许可证。

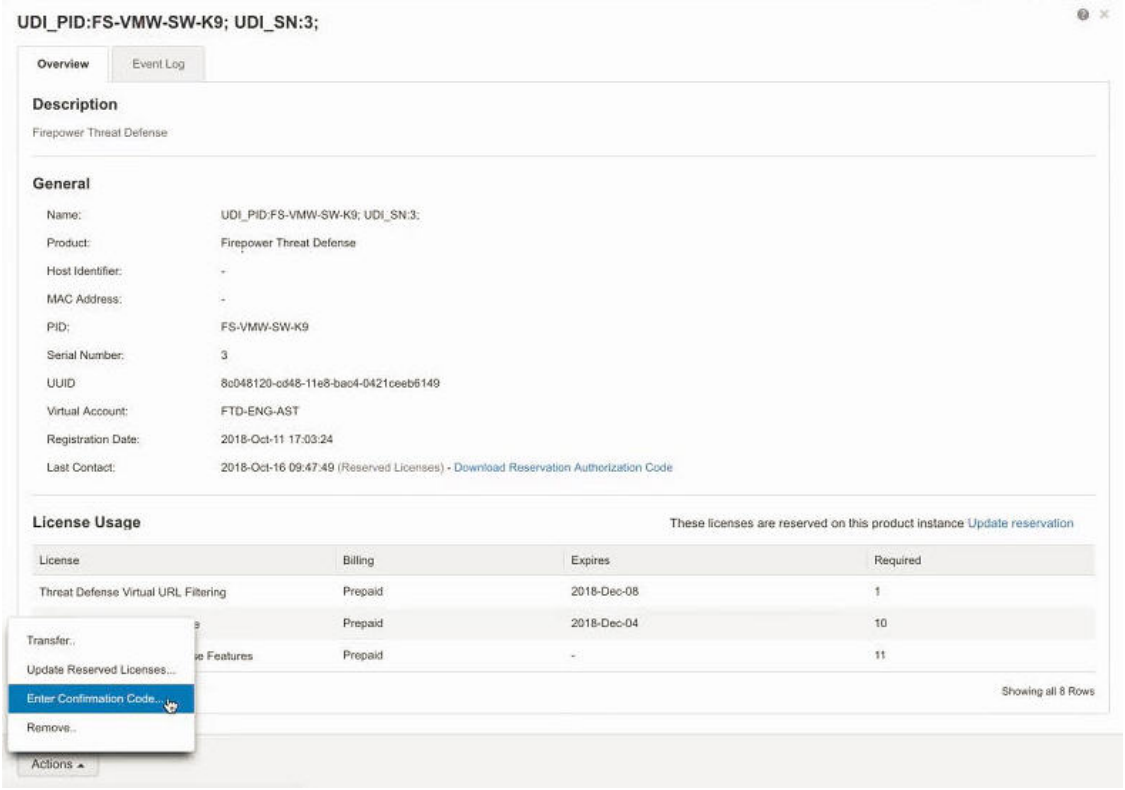
a) 选择**系统** (⚙) > **许可证** > **特别许可证**。
b) 点击**编辑 SLR**。
c) 点击**浏览**以上传新生成的授权码。
d) 点击**安装**以更新许可证。

成功安装授权码后，请确保 防火墙管理中心 **预留** 列中显示的许可证与您在思科智能软件管理器中预留的许可证相匹配。

e) 记下**确认代码**。

步骤 5 在智能软件管理器中输入确认代码：

a) 返回之前在本程序中保持打开状态的智能软件管理器页面。
b) 选择 **操作** > **输入确认代码**：



c) 输入从 防火墙管理中心生成的确认代码。

步骤 6 在 防火墙管理中心中，确认许可证已按照预期予以预留，并且每个受管设备的每个功能均显示带有选中标记 **复选标记**（）的绿色圆圈。

如有需要，请参阅监控特定许可证预留状态，第 45 页了解详细信息。

步骤 7 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》。

停用并归还特定许可证预留

如果不再需要某个特定许可证，则必须将其归还至智能帐户。如果要注册智能许可帐户，必须禁用特定许可证预留（以下程序的步骤 6）。

重要事项 如果不按本程序中的步骤进行操作，则许可证仍会处于使用中的状态，无法重用。

此程序将与 防火墙管理中心关联的所有许可证授权将释放回虚拟账户。注销之后，即不允许对许可的功能进行更新或更改。

过程

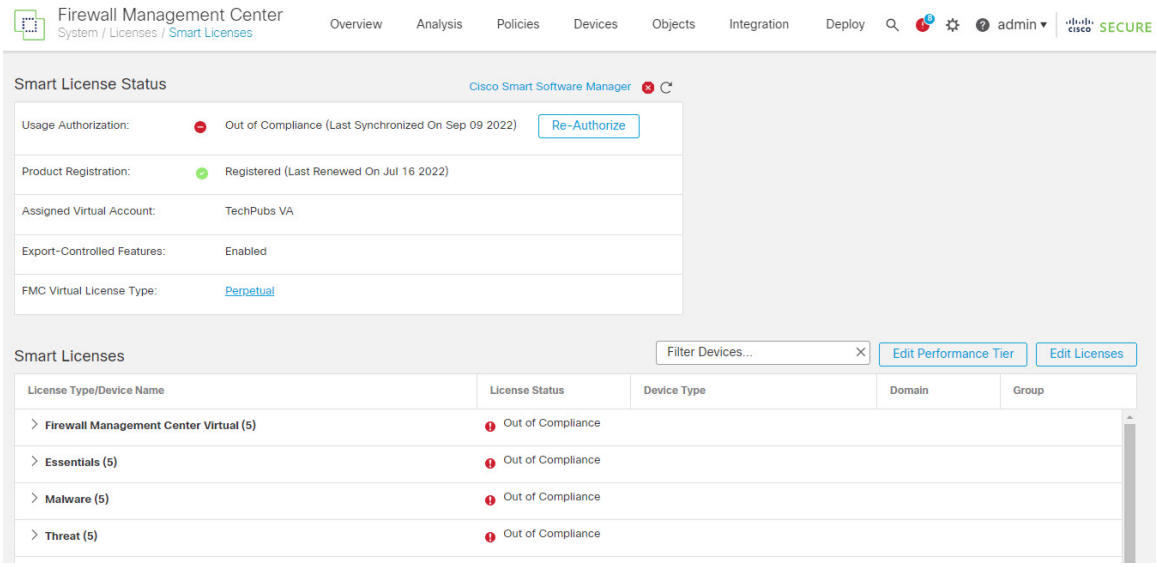
步骤 1 在 防火墙管理中心 Web 界面中，选择 **系统** (⚙) > **许可证** > **特别许可证**。

步骤 2 记下此 防火墙管理中心**产品实例**的标识符。

步骤 3 从 防火墙管理中心生成返还代码，

a) 点击 **返还 SLR**。

下图显示返还 SLR。



设备变为未经许可， 防火墙管理中心 进入取消注册状态。它会生成一个返还代码，并允许您向 SLR 重新注册 防火墙管理中心 。

b) 记下**归还代码**。

步骤 4 在智能软件管理器中，确定要取消注册的 防火墙管理中心 ：

a) 转至智能软件管理器：

https://software.cisco.com/#SmartLicensing-Inventory

b) 如有必要，请点击**清单**。

c) 点击 **产品实例**。

d) 在**类型**列中查找带有**FP**字样的产品实例，并在**名称**列中查找通用SKU（非主机名）。您也可以借助其他表列中的值来确定 防火墙管理中心 是正确的 防火墙管理中心。点击名称。

e) 查看 **UUID** ，看看它是否是您尝试修改的 防火墙管理中心 的 UUID。

如果不是，则必须重复这些步骤，直至找到正确的 防火墙管理中心。

步骤 5 在确定正确的 防火墙管理中心之后，将许可证归还至智能账户：

a) 在显示正确 UUID 的页面上，选择 **操作** > **删除**。

b) 将从 防火墙管理中心 生成的预留归还代码输入 **删除产品实例** 对话框。
c) 点击 **Remove Product Instance**。

特定预留许可证会返回智能账户中的可用池中，而 防火墙管理中心 也会从智能软件管理器产品实例列表中删除。

步骤 6 在 防火墙管理中心 Linux 外壳中禁用特定许可证：

a) 使用 USB 键盘和 VGA 显示器访问 防火墙管理中心 ，或使用 SSH 访问管理界面。
b) 登录 防火墙管理中心 CLI **管理员** 账户。这使您可以访问命令行接口。
c) 输入 **expert** 命令以访问 Linux 外壳。
d) 执行以下命令：

sudo manage_slr.pl

示例：

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) 选择菜单选项 **3** 以禁用特定许可证预留。
f) 选择选项 **0** 退出 manage_slr 实用程序。
g) 输入 **exit** 以退出 Linux 外壳。
h) 输入 **exit** 退出命令行接口。

监控特定许可证预留状态

系统 (⚙) > 许可证 > 特别许可证页面提供 防火墙管理中心 上许可证使用情况的概述，如下所述。

使用授权

可能的状态值包括：

- **已授权** - 防火墙管理中心 符合许可证颁发机构的要求并成功向其注册，该机构已向设备授予许可证授权。
- **不合规** - 如果许可证到期，或者 防火墙管理中心 过度使用许可证（即使它们未被预留），则状态会显示为“不合规”。许可证授权会在特定许可证预留中予以实施，因此必须采取措施。

产品注册

指定授权码上一次在 防火墙管理中心上安装或续订时的注册状态和日期。

出口管制功能

指定是否已为 防火墙管理中心启用出口控制功能。

有关导出控制功能的详细信息，请参阅出口控制功能的许可，第 10 页。

产品实例

此 防火墙管理中心的通用唯一标识符 (UUID)。此值用于在智能软件管理器中标识此设备。

确认代码

如果更新或停用并归还特定许可证，则需要**确认代码**。

“分配的许可证”选项卡

显示分配到每个设备的许可证及其状态。

“预留的许可证”选项卡

显示已使用和可分配的许可证数量，以及许可证到期日期。

特定许可证预留疑难解答

如何在智能软件管理器的产品实例列表中确认某个特定的 防火墙管理中心？

在智能软件管理器的产品实例页面上，如果无法基于表格其中一列中的某个值确认产品实例，则必须点击类型为 **FP** 的每个通用产品实例的名称，以查看产品实例的详细信息页面。此页面上的 **UUID** 值为某个 管理中心的唯一标识。

在 防火墙管理中心 Web 接口中，管理中心 的 UUID 为**系统** (⚙) > **许可证** > **特别许可证**页面上显示的**产品实例**值。

我没有在智能软件管理器中看到许可证预留按钮

如果未看到 **许可证预留** 按钮，则表示您的账户无权使用特定许可证预留。如果已在 Linux 外壳中启用特定许可证预留，并已生成请求代码，请执行以下操作：

1. 如果已在 管理中心 Web 界面中生成 **请求代码**，请取消该请求代码。
2. 在 管理中心 Linux 外壳中禁用特定许可证预留，如停用并归还特定许可证预留，第 43 页部分所述。
3. 使用智能令牌在常规模式下通过思科智能软件管理器注册 管理中心 。
4. 请联系思科 TAC 为您的智能帐户启用特定许可证。

我的许可过程被中断了。如何从中断处继续？

如果已从智能软件管理器生成授权码但尚未下载该授权码，可转至智能软件管理器中的**产品实例**页面，点击产品实例，然后点击 **下载预留授权码**。

我无法将设备注册到 Firewall Management Center Virtual

请在智能账户中确保对想要注册的设备具有足够的 Firewall Management Center Virtual 授权，然后更新部署以添加所需授权。

请参阅更新特定许可证预留，第 41 页。

我已启用特定许可，但看不到智能许可证页面。

这是预期行为。在启用特定许可时，智能许可为禁用状态。您可以使用特定许可证页面来执行许可操作。

如果想要使用智能许可，则必须归还特定许可证。有关详细信息，请参阅停用并归还特定许可证预留，第 43 页。

如果无法在 Firewall Management Center Virtual中看到特定许可证页面怎么办？

您需要启用特定许可证才能查看特定许可证页面。有关详细信息，请参阅启用特定许可菜单选项，第 38 页。

我已禁用特定许可，但忘记复制归还代码。应该怎么办？

返回代码 保存在 Firewall Management Center Virtual中。您必须从外壳重新启用特定许可证（请参阅启用特定许可菜单选项，第 38 页），然后刷新 Firewall Management Center Virtual Web 界面。系统将显示**归还代码**。

配置防火墙管理中心基于 PAK 的旧版许可证

防火墙管理中心支持智能许可证或旧版 PAK（产品激活密钥）许可证作为其平台许可证。此程序介绍如何应用基于 PAK 的许可证。

重新注册智能账户后，您必须为所有经典设备手动添加经典许可证。

开始之前

- 请确保您有思科在您购买许可证时提供的软件索赔证书中的产品激活秘钥(PAK)。如果有延迟，请在获取思科许可证之前联系支持部门。

过程

步骤 1 许可证密钥在智能软件管理器中唯一标识 防火墙管理中心。它由防火墙管理中心的产品代码（例如 66）和管理端口 (eth0) 的 MAC 地址组成；例如，66:00:00:77:FF:CC:88。

a) 选择**系统** (⚙) > **许可证** > **经典许可证**。
b) 点击 **Add New License**。
c) 请记下**添加功能许可证 (Add Feature License)** 对话框顶部的**许可证密钥 (License Key)** 字段中的值。

步骤 2 选择**系统** (⚙) > **许可证** > **经典许可证**。

步骤 3 点击 **Add New License**。

步骤 4 根据情况继续操作：

- 如果您已经获取许可证文本，请跳至步骤 8。
- 如果您仍需要获取许可证文本，请跳至下一步骤。

步骤 5 点击 **获取许可证** ，打开许可证注册门户。

注释
如果无法使用当前的计算机访问互联网，请切换至可访问互联网的计算机，并浏览至http://cisco.com/go/license。

步骤 6 从许可证注册门户中的 PAK 生成一个许可证： https://cisco.com/go/license。

此步骤需要您在购买过程中收到的 PAK 以及 防火墙管理中心的许可证密钥。

有关使用此门户的详细信息，请参阅：

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

您需要帐户凭证才能访问这些链接。

步骤 7 复制许可证注册门户显示或许可证注册门户发送给您的邮件中的许可证文本。

重要事项
门户或邮件中的许可文本块可能包含多个许可证。每个许可证都由一个“开始许可证”行和一个“结束许可证”行来约束。请确保一次仅复制粘贴一个许可证。

步骤 8 返回 Management Center Virtual 的 Web 界面中的**添加功能许可证**页面。

步骤 9 将许可证文本粘贴到**许可证 (License)** 字段。

步骤 10 点击**验证许可证 (Verify License)**。

如果许可证无效，请确保您复制的许可证文本正确无误。

步骤 11 点击**提交许可证 (Submit License)**。

有关许可的其他信息

有关有助于解决许可问题的其他信息，请参阅以下文档：

- 常见问题解答 - 许可常见问题解答

- 许可证路线图

许可证的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
Cisco Secure Firewall Threat Defense 使用指标收集改进功能	7.6.0	任意	Cisco Success Network 和思科支持诊断功能现已默认启用。通过这一增强功能，思科现在可以更有效地从Cisco Secure Firewall Threat Defense 部署中收集遥测数据。 弃用的屏幕：**智能许可产品注册 (Smart Licensing Product Registration)** 页面（**系统 (System)** > **许可证 (Licenses)** > **智能许可证 (Smart Licenses)** > **注册 (Register)**）下的**启用 Cisco Success Network (Enable Cisco Success Network)** 和**启用思科支持诊断 (Enable Cisco Support Diagnostics)** 复选框已被弃用。
智能许可标准化	7.3	任意	我们在防火墙管理中心 GUI 中更改了以下许可证名称： • 基本现在更改为基础版 • 威胁现在更改为 IPS • 恶意软件现在更改为恶意软件防御 • RA VPN/AnyConnect 许可证现在是思科安全客户端 • AnyConnect Plus 现在更改为 Secure Client Advantage • AnyConnect Apex 现在更改为 Secure Client Premier • AnyConnect Apex 和 Plus 现在更改为安全客户端 Premier 和 Advantage • 仅限 AnyConnect VPN 现在更改为仅限 Secure Client VPN
支持运营商许可证	7.3	任意	运营商许可证支持对 Diameter、GTP/GPRS、SCTP 和 M3UA 协议的检测。 新增/修改的屏幕：**系统** > **智能许可证**。
Firewall Threat Defense Virtual智能许可的性能级别	7.0	任意	性能级许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。许可证级别映射到新 Firewall Threat Defense Virtual 型号。

功能	防火墙管理中心最低版本	最低版本	详细信息
Firepower 4100/9300 上多实例功能的许可	6.3	任意	您现在可以在 Firepower 4100/9300 上部署多个 容器实例。每个安全模块/引擎每个功能只需要一个许可证。基础许可证会自动分配给每个实例。 新增/修改的屏幕： **系统** > **许可证** > **智能许可证**。 支持的平台：Firepower 4100/9300 上的
气隙部署的特定许可证预留	6.3	任意	如果客户的部署无法连接互联网以与思科许可证颁发机构通信，则可以使用特定许可证预留。 新/修改后的屏幕： **系统**>**许可证**>**特定许可证**（此选项默认不可用。） 支持的平台：防火墙管理中心、
受限客户的出口控制功能	6.3	任意	如果某些客户的智能账户没有资格使用受限功能，则在获得批准的情况下可以购买基于期限的许可证。 支持的平台：防火墙管理中心、

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。