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 管理中心 支持智能许可证或传统 PAK（产品激活密钥）许可证作为其平台许可证。

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。通过智能软件管理器，您可以为组织创建一个主帐户。

默认情况下，许可证分配给主账户下的默认虚拟账户。作为账户管理员，您可以创建其他虚拟账户；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。

管理中心和设备的许可工作原理

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 管理中心 本身不需要许可证。

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 管理中心 。智能软件管理器会为 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）， 管理中心 可能会从您的账户中删除。

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 管理中心 上的授权，以使更改立即生效。另外，也可以等待 管理中心 按计划通信。

您的 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。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 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 管理中心 在 90 天内联系智能软件管理器，，否则 管理中心 将恢复为未注册状态。

评估模式

在 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， 管理中心 将取消注册。

如果您向智能软件管理器注册 管理中心 ，则评估模式将结束。如果您稍后取消注册 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 3 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。

不合规状态

管理中心 在以下情况下可能会处于不合规状态：

- 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：

- 所有 托管设备许可证 - 操作不受影响。

在您解决许可问题后，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， 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 管理中心
- 与智能软件管理器缺少通信- 管理中心 在 1 年内不与智能软件管理器通信。注意：90 天后， 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 管理中心 ，因此您必须手动重新注册 管理中心。

在未注册状态下， 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 *1:* 智能许可证

您分配的许可证	您购买的订用	持续时间	授予的功能
基本	基于许可证类型	永久或订用 **注释** 基本 订用许可证仅在 Threat Defense Virtual上受支持。	除特定许可证预留和安全防火墙 3100、 基本 永久许可证会自动分配给所有 威胁防御。 用户和应用控制 交换和路由 NAT 有关详细信息，请参阅基本许可证， 第 5 页。
威胁	• T • TC (威胁 + URL) • TMC（ 威胁+恶意软件 防御 + URL）	订用	入侵检测和预防 文件控制 安全情报过滤 有关详细信息，请参阅 威胁许可证， 第 6 页
恶意软件 防御	• TM (威胁 + 恶意软件 防御) • TMC（ 威胁+恶意软件 防御 + URL） • AMP	订用	恶意软件 防御 Secure Secure Malware Analytics 文件存储 有关详细信息，请参阅中的文件和恶意软件策略的许可证要求。恶意软件 防御 许可证， 第 6 页《Cisco Secure Firewall Management Center 设备配置指南》
URL 过滤	• TC (威胁 + URL) • TMC（ 威胁+恶意软件 防御 + URL） • URL	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 7 页。
出口管制功能	无需订用	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 8 页。

您分配的许可证	您购买的订用	持续时间	授予的功能
远程接入 VPN： • AnyConnect Apex • AnyConnect Plus • 仅限 AnyConnect VPN	基于许可证类型	订用或永久	远程接入 VPN 配置。您的账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。 威胁防御 可以使用任何有效 AnyConnect 客户端 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 AnyConnect 客户端许可证，第 7 页 和 《Cisco Secure Firewall Management Center 设备配置指南》中的 *VPN* 许可 。

注释 订用许可证是基于期限的许可证。

基本许可证

基本 许可证允许您：

- 配置您的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 威胁 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。

Secure Firewall 3100

您在购买安全防火墙 3100 时获得 基本 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 管理中心的每个账户， 基本 许可证会自动添加到您的账户。对于特定许可证预留，您需要将 基本 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 威胁 (TM) 或 威胁 和 URL 过滤 (TMC) 订用相结合。

注释 已启用恶意软件防御许可证的受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 管理中心 可以从安全恶意软件分析云接收 Cisco Secure EndpointSecure 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`。

威胁许可证

威胁 许可证可用于执行入侵检测和阻止、文件控制和安全情报过滤：

- 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。
- 安全情报过滤 ， 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情报立即阻止连接。或者，可将“仅监控”设置用于安全情报过滤。

您可以购买 威胁 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：

- 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。
- 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情报信息。
- 在重新启用 威胁之前，您无法重新部署现有入侵策略。

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 服务订用作为独立订用，或与 威胁 (TC) 或威胁和恶意软件防御 (TMC) 订用相结合。

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 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 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 URL 过滤的访问权限。
- 具有 URL 条件的访问控制规则会立即停止过滤 URL。
- 您的 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。

AnyConnect 客户端许可证

您可以使用 AnyConnect 客户端 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： AnyConnect Plus、 AnyConnect Apex 或 仅限 AnyConnect VPN。如果你有 AnyConnect Plus 和 AnyConnect Apex ，并想同时使用这两个许可证，则可以两个都选择。 仅限 AnyConnect VPN许可证不能与 **Apex** 或 **Plus**一起使用。 AnyConnect 客户端 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 AnyConnect 客户端 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）。威胁防御需要强加密（高于 DES），才能与 AnyConnect 客户端 客户端成功建立远程接入 VPN 连接。

如果以下情况属实，则无法部署远程访问 VPN：

- 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
- 远程接入 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：请转至**系统 > 许可证 > 智能许可证**，查看**出口控制功能**是否显示为**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：
- 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 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 管理中心 。

如果在评估模式下或在上 管理中心 启用强加密之前将设备注册到 管理中心，请重新启动每台受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。

Threat Defense Virtual许可证

本部分描述可用于 threat defense virtual 的性能分级许可授权。

可以在任何受支持的 threat defense virtual vCPU/内存配置中使用任何 threat defense virtual 许可证。这可让 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 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 。

Threat Defense Virtual 智能许可的性能级别

RA VPN 的会话限制由安装的 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 *2:* 基于授权的 ***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
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

FTDv 性能级许可准则和限制

许可 threat defense virtual 设备时，请时刻注意以下准则和限制。

- 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 threat defense virtual 核心/内存配置中使用任何 threat defense virtual 许可证。这可让 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 threat defense virtual时选择性能级别。

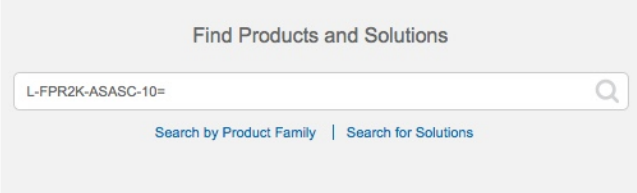
注释 确保智能许可账户包含所需的可用许可证。选择与您账户中的许可证相匹配的级别很重要。如果要将 threat defense virtual 升级到 7.0 版，可以选择 **FTDv - 变量**来保持当前的许可证合规性。threat defense virtual 会根据您的设备功能（内核数/RAM）继续执行会话限制。

- 部署新 threat defense virtual 设备或使用 REST API 调配 threat defense virtual 时，默认性能级别为 FTDv50。
- 基本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 threat defense virtual 设备的 基本 许可证授权，以及 威胁、恶意软件和 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，包括基本许可证。
- 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Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证产品 ID (PID)。

图 *1:* 许可证搜索



Threat Defense Virtual PID

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

- 基本许可证：
  - 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
- 威胁、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

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 1010 PID

- 威胁、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

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 1100 PID

- 威胁、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

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 2100 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-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-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

安全防火墙 3100 PID

- 基本许可证：
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- 威胁、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-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

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 4100 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR4110T-TMC=
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4120T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4140T-TMC=
  - L-FPR4145T-TMC=
  - L-FPR4150T-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-FPR4110T-TMC-1Y
- L-FPR4110T-TMC-3Y
- L-FPR4110T-TMC-5Y
- 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-FPR4120T-TMC-1Y
- L-FPR4120T-TMC-3Y
- L-FPR4120T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4140T-TMC-1Y
- L-FPR4140T-TMC-3Y
- L-FPR4140T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y
- L-FPR4150T-TMC-1Y
- L-FPR4150T-TMC-3Y
- L-FPR4150T-TMC-5Y

- RA VPN - 请参阅 Cisco Secure 客户端订购指南。

Firepower 9300 PID

- 威胁、恶意软件防御和 URL 许可证组合：
  - L-FPR9K-24T-TMC=

- L-FPR9K-36T-TMC=
- L-FPR9K-40T-TMC=
- L-FPR9K-44T-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-24T-TMC-1Y
- L-FPR9K-24T-TMC-3Y
- L-FPR9K-24T-TMC-5Y
- L-FPR9K-36T-TMC-1Y
- L-FPR9K-36T-TMC-3Y
- L-FPR9K-36T-TMC-5Y
- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-44T-TMC-1Y
- L-FPR9K-44T-TMC-3Y
- L-FPR9K-44T-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

- RA VPN - 请参阅思科 AnyConnect 订购指南。

ISA 3000 PID

- 威胁、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

- RA VPN - 请参阅思科 AnyConnect 订购指南。

许可的要求和必备条件

一般前提条件

- 确保在 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 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必备条件

本节介绍 设备高可用性的许可要求。

FTD 服务不支持集群或多实例部署。

设备高可用性许可

高可用性配置中的两台 威胁防御 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，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 基本 许可证和 威胁 许可证，而备用设备只有 基本 许可证， 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 威胁 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 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 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。您可以在 **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **许可证 (License)** 区域中修改集群的许可证。

注释 如果在 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 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。

创建智能账户以保添加许可证

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账户。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账户所需的信息，并确认可以访问该账户。

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 申请智能账户：

有关说明，请参阅https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 。

有关其他信息，请参阅https://communities.cisco.com/docs/DOC-57261。

步骤 2 等待智能账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 3 设置智能账户：

请访问：https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation。

有关说明，请参阅https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604。

步骤 4 验证您是否可以在智能软件管理器中访问该账户。

转至 https://software.cisco.com/#module/SmartLicensing 并登录。

步骤 5 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 10 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。

注册 管理中心 以进行智能许可

您可以通过互联网将 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 管理中心 注册到智能软件管理器

将 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 10 页。

- 确保 管理中心 可以在 tools.cisco.com:443 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 管理中心 相同的机箱 NTP 服务器在机箱上配置 NTP。

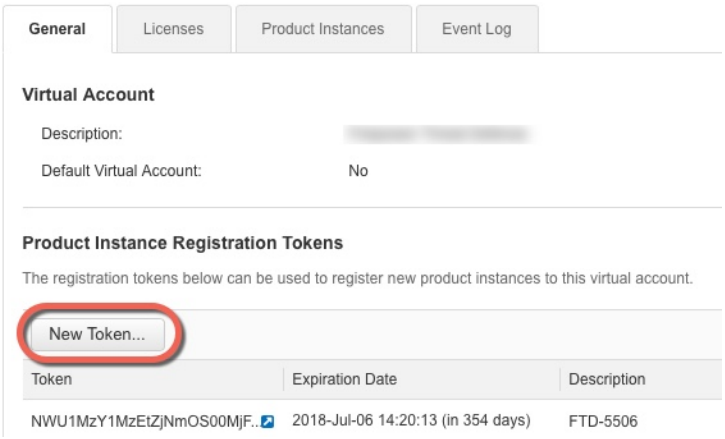
- 如果您的阻止有多个 管理中心，请确保每个 管理中心 拥有唯一的名称，以与可能注册到同一虚拟账户的其他 管理中心 进行区分。此名称对于管理智能许可证授权至关重要，而使用模糊名称稍后会出现问题。

过程

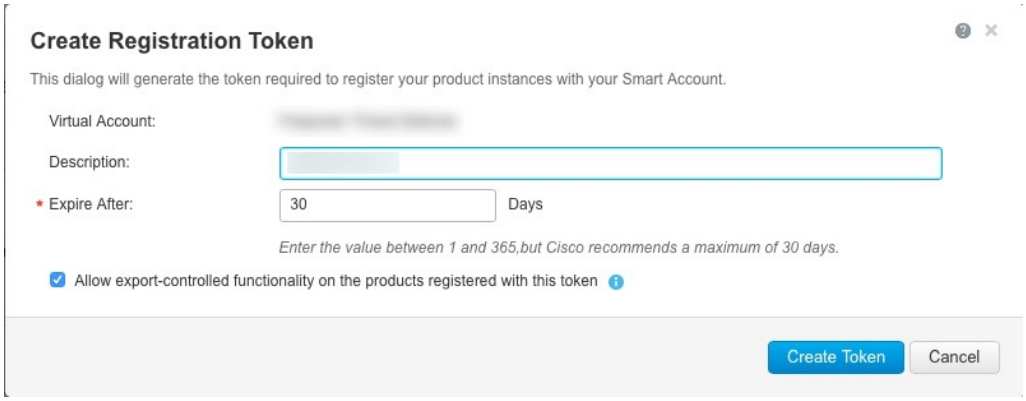
步骤 1 在 智能软件管理器 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

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**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **在使用此令牌注册的产品上允许导出控制的功能 (Allow export-controlled functionality 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。当需要注册威胁防御时，请准备好此令牌，以在该程序后面的部分使用。

图 *2:* 查看令牌

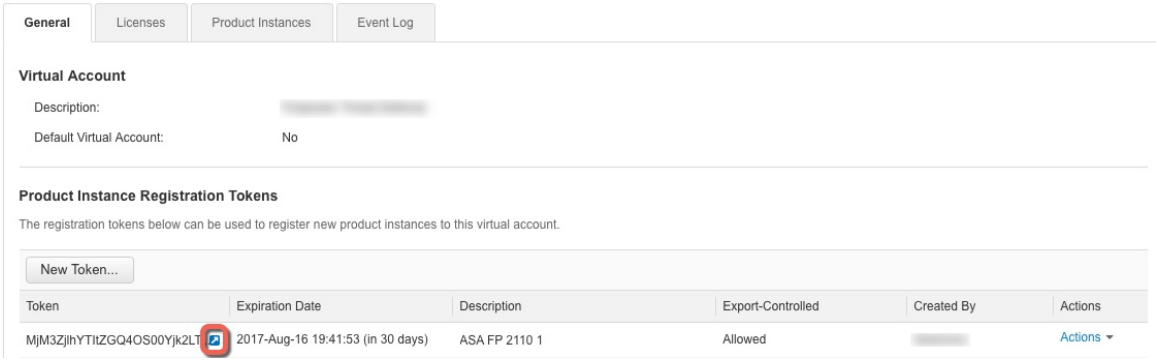
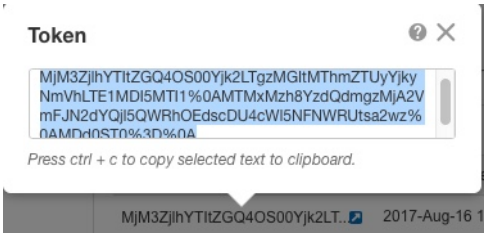


图 *3:* 复制令牌



步骤 2 在 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 点击 **Apply Changes**（应用更改）。

下一步做什么

- 将设备添加到 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 管理中心。

将许可证分配到设备

将设备注册到 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，但如果在受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 对于威胁防御集群，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**（）。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

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 (Save)**。

步骤 7 部署配置更改；请参阅部署配置更改。

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受管设备

受 管理中心 管理的设备通过 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 对于威胁防御集群，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**。

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 23 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 管理中心

从智能软件管理器中取消注册您的管理中心，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 管理中心 或重新映像，请注销。

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 3 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** （🚫）。

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 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 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 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 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 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 管理中心的智能账户下的虚拟账户。如果此部署未关联智能账户内的某个特定虚拟账户，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 8 页。

思科成功网络

指定是否为 管理中心启用了思科成功网络。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。

监控智能许可证

要查看 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 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 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。
- **设备管理** 页面 （**设备 > 设备管理**）列出应用于每个受管设备的许可证。

- **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 。

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 管理中心 具有外部连接。请参阅互联网接入要求。

意外出现不合规通知或其他错误

- 如果设备已向其他 管理中心注册，则需要先注销原始 管理中心 ，然后才能在新的 管理中心下许可该设备。请参阅取消注册 管理中心 ， 第 22 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

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：

- FAQ—https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- 许可证路线图 -https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

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。