为系统授权许可

以下主题介绍如何向 威胁防御设备授予许可证。

防火墙系统的智能许可

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

思科智能软件管理器

在为 威胁防御设备购买一个或多个许可证时，可以在思科智能软件管理器中对其进行管理：https://software.cisco.com/#SmartLicensing-Inventory。通过思科智能软件管理器，您可以为组织创建一个主账户。

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。使用多个虚拟帐户有助于管理大量许可证和设备。

许可证和设备按虚拟帐户进行管理；只有该虚拟帐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帐户传输未使用的许可证。您还可以在虚拟帐户之间传输设备。

当您向思科智能软件管理器注册某个设备时，会在管理器中创建一个产品实例注册令牌，然后将其输入 设备管理器。注册的设备将基于使用的令牌与某个虚拟帐户相关联。

有关思科智能软件管理器的详细信息，请参阅该管理器的在线帮助。

与许可证颁发机构的定期通信

使用产品实例注册令牌注册 威胁防御 设备时，设备会向思科许可证颁发机构注册。许可证颁发机构会为该设备与许可证颁发机构之间的通信颁发 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（通常在九个月或一年内未通信），设备将恢复撤销注册状态，许可的功能将被暂停使用。

设备定期与许可证颁发机构进行通信。如果您在思科智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。另外，也可以等待设备按计划通信。常规许可证通信每 12 小时进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。您必须在 90 天截止前与许可证颁发机构联系。

智能许可证类型

下表介绍了 威胁防御设备可用的许可证。

购买 威胁防御设备会自动附带基本许可证。其他所有许可证均是可选的。

表 *1:* 智能许可证类型

许可证	持续时间	授予的功能
基本	永久	可选期限的许可证中未包括的所有功能。 注册时，基本许可证会自动添加到您的帐户。Cisco Secure Firewall 3100 是个例外。购买防火墙时，您将获得基础许可证，并且该许可证的管理方式与您账户中的其他许可证一样。例如，您需要在注册时确保许可证位于正确的虚拟帐户中。 您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

许可证	持续时间	授予的功能
威胁	基于期限	需要使用以下策略： • 入侵 • 文件（还需要恶意软件） • 安全智能
恶意软件	基于期限	文件策略（还需要 威胁）。
URL	基于期限	URL 策略 - 基于类别和信誉的 URL 过滤或 DNS 查找请求过滤。 您可以对单个 URL 执行 URL 过滤，而不使用此许可证。
RA VPN： • AnyConnect Plus • AnyConnect Apex • 仅限 AnyConnect VPN	基于期限或永久，取决于许可证类型。	远程接入 VPN 配置。您的基础许可证必须允许出口控制功能，以便配置远程访问 RA VPN。在注册设备时，您需要选择是否满足出口要求。 设备管理器 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。如果尚未购买，请参阅远程访问 VPN 的许可要求。 另请参阅《思科 *AnyConnect* 订购指南》http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

Threat Defense Virtual 许可

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

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
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

Threat Defense Virtual 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。
- 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。

出口控制设置对加密功能的影响

注册设备时，您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

评估模式被视为与使用非出口合规账户进行注册相同。这意味着在评估模式下运行时，无法配置远程访问 VPN 或使用高级加密算法。

最特别的是，DES 标准仅在评估或非出口合规模式下可用。

因此，如果您配置加密功能（例如站点间 VPN），或加密高可用性组中的故障转移连接，可能会在注册出口合规账户后最终出现连接问题。如果该功能在评估模式下使用 DES，则在您注册账户后该配置将被破坏。

考虑以下建议来避免与加密相关的问题：

- 在注册设备之前，避免配置加密功能，例如站点间 VPN 和加密的故障转移连接。
- 使用出口合规账户注册设备后，编辑您在评估模式下配置的所有加密功能，并选择更安全的加密算法。测试并验证这些功能中的每项功能，以确保它们正常运行。

注释 如果您在评估模式下配置了 HA 故障转移加密，还需要重新启动 HA 组中的两台设备，才能开始使用更强的加密。建议您先删除加密，以避免两台设备将自己视为主用设备的“脑裂”情况。

可选许可证过期或被禁用的影响

如果以下任一可选许可证过期，您可以继续使用需要该许可证的功能。但是，该许可证将被标记为不合规，您需要购买许可证并将其添加到您的账户，才能使该许可证恢复合规状态。

如果禁用了某个可选许可证，系统将做出如下反应：

- 恶意软件 - 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文件策略，则您无法重新部署这些策略。请注意，在禁用恶意软件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。在时间窗过期后，系统将向这些文件分配不可用的处置情况。
- 威胁 - 系统将不再应用入侵或文件策略。对于安全智能策略，系统不再应用策略并停止下载智能源更新。您无法重新部署需要该许可证的现有策略。
- URL - 带有 URL 类别条件的访问控制规则会立即停止过滤 URL 或 DNS 查找请求，且系统不会再下载对 URL 数据的更新。如果现有访问控制策略包含的规则带有基于类别和信誉的 URL 标准，则不能重新部署现有的访问控制策略。
- RA VPN - 您不能编辑远程访问 VPN 配置，但可以将其删除。用户仍可使用 RA VPN 配置进行连接。但是，如果您更改设备注册，致使系统不再符合导出规定，则远程访问VPN配置会立即停止，且所有远程用户都无法通过 VPN 进行连接。

管理智能许可证

使用“智能许可证”(Smart License) 页面可查看系统当前的许可证状态。系统必须获得许可。

该页面显示您使用的是90天评估许可证，还是已注册到思科智能软件管理器。注册后，您可以查看与思科智能软件管理器的连接状态，以及各类许可证的状态。

使用授权标识智能许可证代理状态：

- 已授权（“已连接”、“足够的许可证”）- 设备已成功联系许可证颁发机构并向其注册，该机构已向设备授予许可证授权。设备现在处于合规状态。
- 不合规 - 设备没有可用的许可证授权。许可功能可继续工作。但您必须购买或释放其他授权，才能变为合规状态。
- 授权已过期 - 设备已连续 90 天或更长时间未与许可颁发机构通信。许可功能可继续工作。在此状态下，智能许可证代理将重试其授权申请。如果重试成功，代理将进入“不合规”或“已授权”状态，并开始新的授权期限。尝试手动同步设备。

注释 点击智能许可证状态旁边的 **i** 按钮，可查看虚拟帐户、出口控制功能，并可获链接来打开思科智能软件管理器。出口控制功能可控制受国家安全、外交政策和反恐怖主义法律和法规约束的软件。

以下步骤程序概述了如何管理系统的许可证。

开始之前

如果您没有系统互联网路径，则无法使用智能许可，而将切换到永久许可证预留 (PLR) 模式。有关详细信息，请参阅在气隙网络中应用永久许可证，第 10 页。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 注册该设备。

只有注册到思科智能软件管理器，才能分配可选许可证。在评估期结束前进行注册。

请参阅注册设备，第 7 页。

注释 注册时，选择是否向思科发送使用数据。可以通过点击齿轮图标旁边的**转到思科成功网络**链接更改选择。

步骤 3 申请和管理可选功能许可证。

只有注册可选许可证后，才能使用该许可证控制的功能。请参阅启用或禁用可选许可证，第 9 页。

步骤 4 维护系统许可。

您可以执行以下任务：

- 与思科智能软件管理器同步，第 9 页

- 取消注册设备，第 10 页

注册设备

购买 威胁防御 设备会自动附带 基本 许可证。基本 许可证涵盖可选许可证未覆盖的所有功能。它是一种永久许可证。

在初始系统设置期间，系统会提示您将设备注册到思科智能软件管理器。如果您选择使用90天的评估许可证，必须在评估期结束前注册设备。

注册设备时，您的虚拟帐户会向设备分配许可证。注册设备也会注册已启用的任何可选许可证。

开始之前

注册设备时，仅该设备被注册。如果设备已配置为高可用性，您必须登录到高可用性对的另一台设备注册该设备。

过程

步骤 1 点击**设备**，然后点击“智能许可证”(the Smart License) 摘要中的**查看配置 (View Configuration)**。

步骤 2 点击**注册设备 (Register Device)**，并按照说明执行操作。

a) 点击链接以打开思科智能软件管理器 (Cisco Smart Software Manager)，然后登录您的账户或创建一个新账户（如果需要）。

b) 生成新的令牌。

在创建令牌时，指定该令牌的有效使用期限。建议的过期期限为 30 天。此期限定义令牌本身的过期日期，不会影响您使用该令牌注册的设备。如果令牌在使用前过期，只需生成一个新令牌即可。

您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

c) 复制该令牌，并将其粘贴到“智能许可证注册”对话框的编辑框中。

d) （**仅限 Threat Defense Virtual**）为您的 threat defense virtual 设备选择性能级别，或保留默认选择。

未选择性能级别时，您的 threat defense virtual 设备将在传统模式下运行，默认设置为 4 核/8 GB；有关详细信息，请参阅更改 Threat Defense Virtual 性能级别，第 8 页。

e) 选择用于思科云服务注册的区域。

注册后，如果需要更改此区域，则必须取消注册该设备，然后重新注册，并选择新区域。

f) 决定是否向思科发送使用数据。

阅读“思科成功网络”步骤中的信息，点击**样本数据 (Sample Data)** 链接查看收集到的实际数据，然后决定是否选中**启用思科成功网络 (Enable Cisco Success Network)** 选项。

g) 点击**注册设备 (Register Device)**。

更改 Threat Defense Virtual 性能级别

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；请参阅Threat Defense Virtual 智能许可的性能级别，第 3 页。

当您将 threat defense virtual 升级到 7.0 以上版本时，设备会自动改为“FTDv 变量”级别状态，并继续使用非分级授权，直到您选择授权级别。

请注意以下事项：

- 您可以根据吞吐量或 RA VPN 要求更改性能级别以满足部署需求。请记住，threat defense virtual 部署时内核和内存资源可调。您选择的性能级别不应超过设备规格。
- AWS 不支持更改性能层。

过程

步骤 1 点击**设备**，然后点击“智能许可证”(the Smart License) 摘要中的**查看配置 (View Configuration)**。

步骤 2 从**性能级别**下拉列表中选择所需选项。

- FTDv5（4 核/8 GB）
- FTDv10（8 核/8 GB）
- FTDv20（8 核/8 GB）
- FTDv30（8 核/16 GB）
- FTDv50（12 核/24 GB）
- FTDv100（16 核/24 GB）

注释 系统根据当前设备规格突出显示最佳级别。

步骤 3 查看您的选择和设备规格。

注释 配置 threat defense virtual VM 时，支持的 vCPU 最大核心数为 12（对于 VMware 和 KVM 上的 FTDv100，最大为 16）；支持的最大内存为 24 GB RAM。您选择的性能级别不应超过设备规格。

步骤 4 点击**是**更改性能级别。

启用或禁用可选许可证

您可以启用（注册）或禁用（解除）可选许可证。只有启用许可证后，才能使用该许可证控制的功能。

如果您不想再使用某个可选期限许可证包含的功能，可以禁用该许可证。禁用许可证会在思科智能软件管理器账户中将其释放，以便可将其应用到其他设备。

另外，在评估模式下运行时，还可启用这些许可证的评估版本。在评估模式下，只有注册设备，许可证才会注册到思科智能软件管理器。但是，您不能在评估模式下启用远程访问 RA VPN许可证。

开始之前

在禁用许可证之前，请确保它不在使用中。重写或删除需要该许可证的任何策略。

对于在高可用性配置中运行的设备，只需在主用设备上上启用或禁用许可证。备用设备请求（或释放）必要许可证时，更改会在下一次部署配置时反映在备用设备上。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。

过程

步骤 1 点击**设备**，然后点击“智能许可证”(Smart License) 摘要中的**查看配置 (View Configuration)**。

步骤 2 根据需要，点击每个可选许可证的**启用/禁用 (Enable/Disable)** 控件。

- **启用** - 将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。

步骤 3 如果启用 **RA VPN** 许可证，请选择您账户中可用的许可证类型。

您可以使用以下任意 AnyConnect 客户端 许可证：**Plus**、**Apex** 或**仅 VPN**。如果您有 **Plus** 和 **Apex** 许可证，并想同时使用它们，则可以两个都选择。

与思科智能软件管理器同步

系统定期与思科智能软件管理器同步许可证信息。常规许可证通信每30天进行一次，但如果设备具有宽限期，则最多运行 90 天，而不会进行自动通报。

不过，如果您在思科智能软件管理器中进行更改，可以刷新设备上的授权，以使更改立即生效。

同步可获取许可证的当前状态，并更新授权和 ID 证书。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 从齿轮下拉列表中选择**重新同步连接**。

取消注册设备

如果您不想再使用设备，可以从思科智能软件管理器中将其取消注册。取消注册后，您的虚拟帐户将释放与该设备关联的基本许可证和所有可选许可证。可选许可证可以分配给其他设备。此外，从云和云服务中取消注册该设备。

取消注册设备后，该设备中的当前配置和策略将继续按原样运行，但无法进行或部署任何更改。

开始之前

当取消注册一台设备时，只有该设备被取消注册。如果该设备已配置高可用性，那么您必须登录到高可用性对的另一台设备才能取消注册该设备。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 从齿轮下拉列表中选择**取消注册设备**。

步骤 3 如果确实要取消注册设备，请阅读警告并点击**取消注册**。

在气隙网络中应用永久许可证

气隙网络是指内部没有通往互联网的路径的网络。这些网络是高安全性网络，您希望在其中消除任何外部进入和攻击的可能性。由于没有通往互联网的路径，因此您无法直接在思科智能软件管理器中注册设备。但是，您可以使用永久许可证预留 (PLR) 模式来获取可应用于设备的许可证。

如果需要使用 PLR 模式，请注意以下几点：

- 需要接入互联网的功能（例如文件策略、URL 查找或对公共网站的上下文交叉启动）将无法工作。
- 即使您启用了网络分析和思科成功网络，思科也不会由于缺少互联网访问权限而收集相关数据。
- 您需要手动上传地理位置数据库、入侵规则和漏洞数据库 (VDB) 的更新。例如，可以将更新下载到闪存，然后将闪存放入您的安全建筑物中，并从受保护的工作站上传更新。

注释 思科智能软件管理器使用设备序列号来分配永久许可证。如果您需要取消注册设备，并且正常的取消注册或取消过程无法删除许可证分配，则需要联系思科技术支持部门，以从思科智能软件管理器中删除注册。重新映像设备不会删除许可证注册。

以下主题详细介绍不同类型的永久许可证及其应用方式，以及如何取消注册或取消注册设备。

通用永久与特定许可证预留

有两种不同类型的许可证预留：

- 通用永久许可证预留（通用 PLR 或 UPLR）- 通用永久许可证允许永久无限制地使用受支持防火墙产品，其中包括所有可选许可证。在您购买并应用通用永久许可证后，任何已应用的功能许可证（通常是基于时间的许可证）都将永久适用。但是，智能许可证账户中的替换许可证到期时，您仍需购买替换许可证。
- 特定许可证预留-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。当您获取此许可证时，可以选择除基本许可证外的所需可选功能许可证。必须在许可证到期时定期更新许可证。

设备管理器 仅支持通用 PLR。

您必须与思科代表协作，在自己的思科智能软件管理器 (CSSM) 账户中启用“通用永久许可证预留”(PLR) 模式。

验证您的智能账户是否可以提供通用许可证

要验证您是否可以获取和应用永久许可证，请登录 CSSM 账户并转至**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)**页面，然后点击**许可证 (Licenses)** 选项卡。如果您可以看到**许可证预留**按钮，则表明您有权获取永久许可证预留。

但是，此按钮会启动一个同时适用于通用和特定永久许可证的向导。

您还必须完整查看可用许可证列表，以验证是否存在适用于设备的通用许可证。此许可证将在由**许可证预留**按钮启动的向导的第 2 步中显示为可选项。

如果您可以看到**许可证预留**按钮，并且可以获取通用许可证，则可以继续转换系统以使用永久许可证。如果未显示此按钮，或者您只能预留特定许可证，请致电您的思科代表，并请求为您的账户启用通用 PLR 模式。

切换到 PLR 模式并应用通用许可证

如验证您的智能账户是否可以提供通用许可证，第 11 页中所述，一旦您确认自己可以获取永久许可证并已购买所需的通用许可证，就可以切换到永久许可证预留 (PLR) 模式并应用许可证。

⚠

注意 如果您当前处于评估模式，则在切换到 PLR 模式后无法切换回评估模式。

开始之前

如果设备配置为具有高可用性，则必须为高可用性组中的两个设备单独完成此任务。

过程

步骤 1 点击**设备**，然后点击智能许可证摘要中的**查看配置**。

步骤 2 如果您已使用智能许可功能注册设备，请从齿轮⚙下拉列表中选择**取消注册设备**，然后确认取消注册。等待注销任务完成，然后再继续操作。

步骤 3 从齿轮⚙下拉列表中选择**切换到通用 PLR**，以切换到“通用永久许可证预留”(PLR) 模式。

阅读警告信息，然后点击**是**确认切换。

系统将转换为 PLR 模式，然后开始 PLR 注册过程。

步骤 4 完成 PLR 注册。

a) 当系统打开“通用永久许可证预留”对话框时，第一步中包括您将需要的请求代码。您可以点击**另存为 TXT** 将其保存在文本文件中，或点击**打印**将其打印出来。您还可以突出显示字符串，然后按 Ctrl+C 将字符串复制到剪贴板。

如果您在切换模式后取消进程，可以点击“许可”(Licensing) 页面上的**继续预留 (Continue Reservation)** 按钮来重启。

b) 登录您的 CSSM 账户，转到**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)**页面，然后点击**许可证 (Licenses)**选项卡。

c) 点击**许可证预留**按钮，然后按照向导中的说明进行操作。系统将提示输入您生成的请求代码，然后，您将获得授权码。

该向导包括以下步骤：

1. 输入许可证请求代码，或上传含代码的文本文件，然后点击**下一步**。
2. 在第 2 步中，系统将显示您将许可的系统的产品详细信息，以及可用许可证的项目符号列表。为本地管理的 威胁防御 设备选择通用许可证，然后点击 **下一步**。
3. 在第 3 步中，验证您是否选择了正确的许可证，然后点击**生成授权码**。
4. 在第 4 步中，系统将显示授权码。点击**下载为文件**或**复制到剪贴板**，以保存代码。
5. 点击**关闭**以退出向导。

d) 返回 设备管理器，将授权码粘贴到相应的字段中。

通用许可证的有效授权码的格式为 XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX，其中 X 是字母数字字符。如果您的授权码是 XML 文件，则表示您具有特定许可证，并且不能在

此系统上使用该许可证。请如取消 PLR 注册，第 13 页中所述取消注册，以确保在 CSSM 中发布预留许可证。然后，与思科代表合作，将您的智能账户转换为通用 PLR。

e) 点击**注册**。

系统将开始注册过程。刷新“许可”(Licensing) 页面以检查注册状态。

步骤 5 根据需要启用可选功能许可证。

通用许可证仅为设备注册 基本 许可证。现在，您可以为每个所需功能许可证点击**启用**。

取消 PLR 注册

在完成前，您可以取消“通用永久许可证预留 (PLR)”请求。例如，如果您启动 PLR 注册流程，并发现您的智能软件管理器账户未设置 PLR，则您可以在获得 PLR 模式的授权和适当设置智能许可证账户时取消此流程。

如果已完成 PLR 注册流程，则无法取消此流程。请参阅在 PLR 模式下取消注册设备，第 14 页。

过程

步骤 1 点击**设备**，然后点击智能许可证摘要中的**查看配置**。

步骤 2 从齿轮 下拉列表中选择**取消 PLR**，以开始取消流程。

步骤 3 选择适用于您的选项：

- **我在 CSSM 中有许可证** - 如果您已通过思科智能软件管理器 (CSSM) 中的许可证注册向导，并且已获得授权码，请使用此选项。此时，CSSM 中预留有许可证，您需要释放这些许可证。
- **我在 CSSM 中没有许可证** - 如果您在获取授权码时尚未完成 CSSM 向导，则使用此选项。例如，如果您在 设备管理器 中启动 PLR 注册，但随后发现您的智能账户中没有显示 **许可证预留** 按钮。

步骤 4 （如果已选择**我在 CSSM 中有许可证**。）您需要从 CSSM 获取释放码，以确保您的许可证不再被标记为正在使用。否则，其他设备将无法使用这些许可证。

a) 将您从 CSSM 获取的授权码（在注册时）粘贴到取消对话框，然后点击**生成释放码**。

b) 当**释放许可证代码**字段中有代码时，点击**另存为 TXT** 将其保存到文本文件，或点击**打印**进行打印。您还可以选择代码，然后按 Ctrl+C 将其复制到剪贴板。

c) 在 CSSM 中，在**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)** 页面中找到设备（名称是设备序列号），点击**操作 (Action)** > **删除 (Remove)**，然后输入释放码。

等待 CSSM 指示产品已成功删除。

步骤 5 点击**确定**完成取消流程。

系统将返回到“智能许可证”模式。但是，设备将被取消注册，并且您无法重启评估模式。此时，您必须使用智能许可证来注册设备，或切换回 PLR 模式并重新注册，才能使用该设备。

在 PLR 模式下取消注册设备

如果不再需要对设备进行许可（例如，因为要停用设备或将其移至另一个需单独许可的设备），则可以取消注册该设备。

取消注册设备时会将许可证恢复为未使用状态。如果不取消注册设备，许可证仍将标记为正在使用中，并且不能用于其他用途。

过程

步骤 1 点击**设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 从齿轮 下拉列表中选择**取消注册通用 PLR**，阅读警告信息，然后点击**是**开始此流程。

步骤 3 当“取消注册通用永久许可证预留”对话框打开时，系统将在**发布许可证代码**字段中填充您在发布 CSSM 账户中当前已分配许可证所需的代码。点击**另存为 TXT**，或点击**打印**以保留此代码的副本。您也可以选择此项并使用 Ctrl+C 将其复制到剪贴板。

步骤 4 转到您的 CSSM 账户，在**智能软件许可 (Smart Software Licensing)** > **清单 (Inventory)**页面中找到设备（“名称”(Name) 是设备序列号），点击**操作 (Action)** > **删除 (Remove)**，然后输入释放码。

等待 CSSM 指示产品已成功删除。

步骤 5 返回 设备管理器，在“取消注册设备”对话框中点击 **取消注册** 。

由此，此过程便已完成。此时，CSSM 中的许可证可分配给其他设备，并且 威胁防御 设备未经许可。

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。