许可证：智能软件许可

通过智能软件许可，您可以集中购买和管理许可证池。与产品授权密钥 (PAK) 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASA，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。

注释 有关每个平台的智能许可功能和行为的详细信息，请参阅支持智能的产品系列。

关于智能软件许可

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

Firepower 4100/9300 机箱上 ASA 的智能软件许可

对于 Firepower 4100/9300 机箱上的 ASA，智能软件许可配置，划分为 Firepower 4100/9300 机箱管理引擎和 ASA 两部分。

- Firepower 4100/9300 机箱- 在机箱上配置所有智能软件许可基础设施，包括用于与智能软件管理器进行通信的参数。Firepower 4100/9300 机箱本身无需任何许可证即可运行。有关 CLI 操作步骤，请参阅《FXOS 配置指南》。

注释 机箱间集群需要您在集群的每个机箱上启用相同的智能许可方法。

- ASA 应用 - 在 ASA 中配置所有许可证授权。

智能软件管理器和账户

在为设备购买一个或多个许可证时，可在思科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。

注释 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，您可以选择创建其他虚拟账户；例如，您可以为区域、部门或子公司创建账户。通过多个虚拟账户，您可以更轻松地管理大量许可证和设备。

离线管理

如果您的设备无法访问互联网，也不能向智能软件管理器注册，您必须配置离线许可。

永久许可证预留

如果您的设备出于安全原因而无法访问互联网，您可以选择为每个ASA请求永久许可证。永久许可证不需要定期访问智能软件管理器。与 PAK 许可证一样，您可以购买许可证并为 ASA 安装许可证

密钥。与PAK许可证不同的是，您可以通过智能软件管理器获取和管理许可证。您可以在定期智能许可模式与永久许可证预留模式之间轻松切换。

注释 ASA 不支持特定许可证预留 (SLR)。在 SLR 中，特定功能授权将永久启用。ASA 仅支持永久启用所有功能的 PLR。

ASA Virtual 永久许可证预留

注释 仅在 VMware 和 KVM 上支持永久许可证预留。

您可以获得启用以下所有功能的型号特定许可证：

- 模式的最大吞吐量
- 基础 层
- 强加密 (3DES/AES) 许可证，如果您已在智能许可账户中启用该功能
- 为平台启用的 Secure Client 功能

注释 能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

Cisco 提供两种永久许可证保留模式ASA Virtual：

- 基于内存和 vCPU 的永久许可证预留模式
- 灵活永久许可证预留模式

基于内存和 vCPU 的永久许可证预留模式

您可以根据分配给 ASA Virtual 的 RAM 和 vCPU 来配置型号特定许可证。例如，具有 8 GB RAM 和 4 个 vCPU 的 ASA Virtual 始终使用具有 2G 吞吐量的 ASAv30 许可证。

vCPU 和内存与许可证的关系如下：

- 2 GB，1 个 vCPU - ASAv5 (100M)（必须运行 **license smart set_plr5** 命令；否则，ASAv10 许可证会分配为允许 1 G 吞吐量。）

注释 在版本 9.13 中，ASAv5 RAM 要求被提高到了 2 GB。由于 RAM 的增加，ASAv5 永久许可证不再有效，因为 ASA 检查了分配的内存并确定 2 GB RAM 实际上是 ASAv10，而不是 ASAv5。要允许 ASAv5 永久许可证工作，您必须将 ASA 配置为为此模式识别额外的内存。

- 2 GB，1 个 vCPU - ASAv10 (1G)
- 8 GB，4 个 vCPU - ASAv30 (2G)
- 16 GB，8 个 vCPU - ASAv50 (10G)
- 32 GB，16 个 vCPU - ASAv100 (20G)
- 64 GB，32 个 vCPU - ASAvU
- 128 GB，64 个 vCPU - ASAvU

稍后，如果要更改设备的型号级别，则必须退回当前许可证并在正确的型号级别请求新的许可证。要更改已部署的 ASA Virtual 的型号，在虚拟机监控程序中，可以更改 vCPU 和 DRAM 设置以匹配新的型号要求。有关这些值，请参阅《*ASA Virtual Virtual 入门指南*》。

如果您停止使用许可证，则必须通过在 ASA Virtual 上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。您必须正确遵循退回过程，以避免为未使用的许可证付费。

灵活永久许可证预留模式

您可以配置任何型号特定许可证，而不考虑分配给 ASA Virtual 的RAM 和 vCPU。

您指定的型号许可证会设置 ASA Virtual 的吞吐量水平。您的 ASA Virtual 的内存将决定最大 Secure Client、TLS 代理会话数、最大并发防火墙连接数和 VLAN 数。但是，较低的 ASA Virtual 内存配置文件将限制实际的会话和功能数量。

例如，如果 ASA Virtual 具有 8 GB RAM 并向 ASAV_50_UNIVERSAL 注册，则分配的最大 Secure Client 会话数为 750。当会话超过此限制时，系统就会丢弃这些连接。

此永久许可证预留许可证模式的其他优势包括：

- 您可以在永久许可证预留许可证之间切换，而不考虑分配给 ASA Virtual 的内存。但是，如果 ASA Virtual 的vCPU 超过 16 个，则您只能配置 ASAvU（无限）许可证。
- 您可以更改分配给 ASA Virtual 的内存和 vCPU，而无需更改型号许可证。

如果您停止使用许可证，则必须通过在 ASA Virtual 上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。您必须正确遵循退回过程，以避免为未使用的许可证付费。

有关配置永久许可证预留的详细信息，请参阅ASA Virtual：配置永久许可证预留 ，第 42 页。

Firepower 1010 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- Security Plus
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Firepower 1100 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 最大安全情景数
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Cisco Secure Firewall 1210/1220 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 最大安全情景数
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Cisco Secure Firewall 1230/1240/1250 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 最大安全情景数
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Cisco Secure Firewall 3100/4200 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 最大安全情景数
- 运营商许可证
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Firepower 4100/9300 机箱永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层。
- 最大安全情景数
- 运营商许可证
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

注释 许可证在 Firepower 4100/9300 机箱上管理，但您还需要请求 ASA 配置授权，以便 ASA 允许使用它们。管理许可证，请参阅《FXOS 配置指南》。

如果您停止使用许可证，则必须通过在 Firepower 4100/9300 机箱 上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

智能软件管理器本地版

如果您的设备出于安全原因无法访问互联网，您可以选择以虚拟机 (VM) 形式安装本地智能软件管理器卫星（也称为“智能软件卫星服务器”）服务器。该本地智能软件管理器提供智能软件管理器功能的子集，并允许您为所有本地设备提供必要的许可服务。只有本地智能软件管理器需要定期连接到主智能软件管理器，才能同步您的许可证使用情况。您可以按时间表执行同步，也可以手动同步。

您可以在本地智能软件管理器上执行以下功能：

- 激活或注册许可证
- 查看公司的许可证
- 在公司实体之间传输许可证

有关更多信息，请参阅思科智能软件管理器本地部署产品手册。

按虚拟帐户管理的许可证和设备

仅当虚拟账户可以使用分配给该账户的许可证时，才能按虚拟账户对许可证和设备进行管理。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。

对于 Firepower 4100/9300 机箱上的 ASA - 仅机箱注册为设备，而机箱中的 ASA 应用会请求自己的许可证。例如，对于配有 3 个安全模块的 Firepower 9300 机箱，机箱计为一个设备，但模块使用 3 个单独的许可证。

评估许可证

ASA Virtual

ASA Virtual 不支持评估模式。在 ASA Virtual 向智能软件管理器注册之前，它会在严格限制速率的状态下运行。

Firepower 1000

在 Firepower 1000 向智能软件管理器注册之前，它会在评估模式下运行 90 天（总用量）。仅已启用默认授权。当此期限结束时，Firepower 1000 将变为不合规。

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。

Firepower 2100

在 Firepower 2100 向智能软件管理器注册之前，它会在评估模式下运行 90 天（总用量）。仅已启用默认授权。当此期限结束时，Firepower 2100 将变为不合规。

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。

Cisco Secure Firewall 3100/4200

在 Cisco Secure Firewall 3100/4200 向智能软件管理器注册之前，它会在评估模式下运行 90 天（总使用量）。仅已启用默认授权。当此期限结束时，Cisco Secure Firepower 3100/4200 将变为不合规。

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。

Firepower 4100/9300 机箱

Firepower 4100/9300 机箱支持两种类型的评估许可证：

- 机箱级评估模式 - 在 Firepower 4100/9300 机箱 向智能软件管理器注册之前，会在评估模式下运行 90 天（总使用量）。ASA 在此模式下无法请求特定授权，只能启用默认授权。当此期限结束时，Firepower 4100/9300 机箱会变为不合规。
- 基于授权的评估模式 - 在 Firepower 4100/9300 机箱向智能软件管理器注册之后，您可以获取基于时间的评估许可证，并可将这些许可证分配给 ASA。在 ASA 中，可照常请求授权。当该基于时间的许可证到期时，您需要续订基于时间的许可证或获取永久许可证。

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并获取永久许可证，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

关于按类型划分的许可证

以下部分包括有关按类型分类的许可证的其他信息。

Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证

Secure Client 许可证不会直接应用于 ASA。但是，您需要购买许可证并将其添加到您的智能账户，以保证将 ASA 用作 Secure Client 前端。

- 对于 Secure Client Advantage 和 Secure Client Premier 许可证，将您打算在智能账户中的所有 ASA 中使用的对等体数量相加，并为该数量的对等体购买许可证。
- 对于 仅限 Secure Client VPN，请为每个 ASA 购买一个许可证。与提供可由多个 ASA 共享的对等体池的其他许可证不同， 仅限 Secure Client VPN 许可证是按前端划分的。

有关详情，请参阅：

- Cisco Secure Client 订购指南
- Secure Client 许可常见问题解答 (FAQ)

其他 VPN 对等体数

其他 VPN 对等体包括以下 VPN 类型：

- 使用 IKEv1 的 IPsec 远程访问 VPN
- 使用 IKEv1 的 IPsec 站点间 VPN
- 使用 IKEv2 的 IPsec 站点间 VPN

此许可证包含在基础许可证中。

VPN 对等体总数，所有类型

- VPN 对等体总数是 Secure Client 和其他 VPN 对等体允许的最大 VPN 对等体数。例如，如果总数为 1000，则可以同时允许 500 个 Secure Client 和 500 个其他 VPN 对等体；或 700 个 Secure Client 和 300 个其他 VPN；或对 Secure Client 使用全部 1000 个。如果超出了 VPN 对等体总数，可以对 ASA 实施过载，以确保相应地调整网络大小。

加密许可证

强加密：**ASA Virtual**

在连接到智能软件管理器或智能软件管理器本地服务器之前，强加密 (3DES/AES) 可用于管理连接，因此您可以启动 ASDM 并连接到智能软件管理器。对于需要强加密（如 VPN）的通过设备的流量，在您连接到智能软件管理器并获得强加密许可证之前，吞吐量会受到严格限制。

当您向智能软件许可帐户请求 ASA Virtual 的注册令牌时，请选中 **允许在通过此令牌注册的产品上使用导出控制功能** 复选框，以便应用强加密 (3DES/AES) 许可证（您的帐户必须符合其使用条件）。如果 ASA Virtual 之后变为不合规状态，只要已成功应用导出合规性令牌， ASA Virtual 将会保留许可证，并且不会恢复到速率受限状态。如果您重新注册 ASA Virtual，并且禁用了导出合规性，或者如果您将 ASA Virtual 还原到出厂默认设置，系统将会删除该许可证。

如果最初注册 ASA Virtual 时未使用强加密，之后又添加了强加密，则必须重新加载 ASA Virtual 才能使新许可证生效。

对于永久许可证预留许可证，如果您的帐户符合使用条件，则启用强加密 (3DES/AES) 许可证。

如果您的智能账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账户。

强加密：设备模式下的 **Firepower 1000**、**Cisco Secure Firewall 1200/3100/4200**

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到智能软件管理器，还可以立即使用 ASDM。如果之后在 ASA 上配置了 SSH 访问，也可以使用 SSH 和 SCP。其他需要强加密（例如 VPN）的功能必须启用强加密，这要求您先向智能软件管理器注册。

注释 如果您在注册之前尝试配置任何可使用强加密的功能（即使您仅配置了弱加密），您的 HTTPS 连接会在该接口上断开，并且您无法重新连接。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。如果您丢失了 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅管理接口，或者连接到没有为强加密功能配置的接口。

当您向智能软件许可帐户请求 ASA 的注册令牌时，请选中 **允许在通过此令牌注册的产品上使用导出控制功能** 复选框，以便应用强加密 (3DES/AES) 许可证（您的帐户必须符合其使用条件）。如果 ASA 之后变为不合规状态，只要已成功应用导出合规性令牌，ASA 将会继续允许通过设备的流量。即使您重新注册 ASA 并禁用导出合规性，许可证仍将保持启用状态。如果您将 ASA 恢复到出厂默认设置，系统将会删除该许可证。

如果最初注册 ASA 时未使用强加密，之后又添加了强加密，则必须重新加载 ASA 才能使新许可证生效。

对于永久许可证预留许可证，如果您的帐户符合使用条件，则启用强加密 (3DES/AES) 许可证。

如果您的智能账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账户。

强加密：Firepower 4100/9300 机箱

当ASA部署为逻辑设备时，您可以立即启动ASDM。在您连接并获取强加密许可证之前，不允许通过需要强加密（如 VPN）设备的流量。

当您向智能软件许可帐户请求机箱的注册令牌时，请选中 **允许在通过此令牌注册的产品上使用导出控制功能** 复选框，以便应用强加密 (3DES/AES) 许可证（您的帐户必须符合其使用条件）。

如果 ASA 之后变为不合规状态，只要已成功应用导出合规性令牌，ASA 将会继续允许通过设备的流量。如果您重新注册机箱，并且禁用了导出合规性，或者如果您将机箱还原到出厂默认设置，系统将会删除该许可证。

如果最初注册机箱时未使用强加密，之后又添加了强加密，则必须重新加载ASA应用程序才能使新许可证生效。

对于永久许可证预留许可证，如果您的帐户符合使用条件，则启用强加密 (3DES/AES) 许可证。

如果您的智能账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账户。

DES：所有型号

如果启用了强加密，则无法使用 DES。

运营商许可证

借助运营商许可证，可以实现以下检查功能：

- 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 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）。M3UA 在 RFC 4666 中定义。
- RFC 4960 中介绍了 SCTP—SCTP（流控制传输协议）。该协议支持基于 IP 的电话信令协议 SS7，也是适用于 4G LTE 移动网络架构中多个接口的传输协议。

TLS 代理会话总数

用于加密语音检测的每个 TLS 代理会话都会计入 TLS 许可证限制中。

使用 TLS 代理会话的其他应用不计入 TLS 限制，例如移动性优势代理（无需许可证）。

某些应用可能会在一个连接中使用多个会话。例如，如果为一部电话配置了主用和备用思科 Unified Communications Manager，则有 2 个 TLS 代理连接。

使用 **tls-proxy maximum-sessions** 命令，或在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格，单独设置 TLS 代理限制。要查看型号的限制，请输入 **tls-proxy maximum-sessions ?** 命令。如果应用的 TLS 代理许可证高于默认的 TLS 代理限制，则 ASA 自动设置 TLS 代理限制以与许可证匹配。TLS 代理限制的优先级高于许可证限制；如果设置的 TLS 代理限制低于许可证限制，则无法使用许可证中的所有会话。

注释 对于以“K8”结尾的许可证部件号（例如，用户数少于 250 的许可证），TLS 代理会话数限制为 1000。对于以“k9”结尾的许可证部件号（例如，用户数为 250 或更多的许可证），TLS 代理限制取决于配置，最高值为型号限制。K8 和 K9 是指许可证是否有出口限制：K8 不受限制，K9 受限制。

如果清除配置（例如使用 **clear configure all** 命令），TLS 代理限制将设置为模型的默认值；如果默认值低于许可证限制，会显示一条错误消息，让您使用 **tls-proxy maximum-sessions** 命令再次增加该限制（在 ASDM 中，使用 **TLS Proxy** 窗格）。如果使用故障转移并输入 **write standby** 命令，或者在 ASDM 中，在主设备上使用 **File > Save Running Configuration to Standby Unit** 来强制进行配置同步，则会在辅助设备上自动生成 **clear configure all** 命令，因此，您可能会在辅助设备上看到警告消息。由于配置同步会恢复在主设备上设置的 TLS 代理限制，因此可以忽略该警告。

您也可能为连接使用 SRTP 加密会话：

- 对于 K8 许可证，SRTP 会话数限制为 250。
- 对于 K9 许可证，则没有任何限制。

注释 只有需要对媒体进行加密/解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通式，即使两端均为 SRTP，这些呼叫也不计入限制。

最大 VLAN 数量

对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。 例如：

```
interface gigabitethernet 0/0.100
vlan 100
```

僵尸网络流量过滤器许可证

要下载动态数据库，需要强加密 (3DES/AES) 许可证。

故障转移或 ASA 集群许可证

ASAv 的故障转移许可证

备用设备需要与主设备相同型号的许可证。

Firepower 1010 的故障转移许可证

智能软件管理器常规版和本地版

两台 Firepower 1010 设备都必须向智能软件管理器或智能软件管理器本地服务器注册。两台设备都要求您先启用基础许可证和安全加许可证，然后才能配置故障转移。

通常，您也不需要在 ASA 中启用强加密（3DES/AES）功能许可证，因为在注册设备时，两台设备都应获得强加密令牌。使用注册令牌时，两台设备必须具有相同的加密级别。

如果您的智能账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账户。在这种情况下，请在启用故障转移后在主用设备上启用它。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。只有主用设备需要向服务器请求许可证。许可证将聚合为一个单独的故障转移许可证，供该故障转移对共享，并且此聚合许可证还将缓存在备用设备上，以便在该设备将来成为主用设备时使用。在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，且没有使用强加密令牌，则将无法对需要强加密 (3DES/AES) 功能许可证的功能进行配置更改；否则操作不会受到影响。新主用设备每隔35秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Firepower 1100 的故障转移许可证

智能软件管理器常规版和本地版

只有主用设备需要向服务器请求许可证。许可证聚合为故障转移对共享的单个故障转移许可证。辅助设备不会产生额外成本。

为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

注释 每个 ASA 在形成故障转移对时必须具有相同的加密许可证。将 ASA 注册到智能许可服务器时，当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。由于此要求，在使用具有故障转移功能的强加密令牌时，您有两种许可选择：

- 在启用故障转移之前，请将两台设备注册到智能许可服务器。在这种情况下，两台设备将具有强加密功能。然后，在启用故障转移后，继续在主用设备上配置许可证授权。如果为故障转移链路启用加密，系统将会使用 AES/3DES（强加密）。
- 在将主用设备注册到智能许可服务器之前，请启用故障转移。这种情况下，两台设备都还不能进行强加密。然后，配置许可证授权并将主用设备注册到智能许可服务器；两台设备都将从聚合许可证中获得强加密。请注意，如果您在故障转移链路上启用了加密，系统将使用 DES（弱加密），因为故障转移链路是在设备获得强加密之前建立的。您必须重新加载两台设备，才能在链路上使用 AES/3DES。如果仅重新加载一台设备，则该设备将尝试使用 AES/3DES，而原始设备则使用 DES，这将导致两台设备变为活动状态（脑裂）。

各个插件许可证类型将按以下方式进行管理：

- 基础—虽然只有主用设备需要向服务器请求此许可证，但默认情况下备用设备已启用了基础许可证；它不需要向服务器注册来使用它。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1120 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 3 个情景的许可证。因此，聚合故障转移许可证包括 7 个情景。不过，由于一台设备的平台限制为 5，因此合并许可证最多仅允许 5 个情景。在此情况下，只能将主用情景许可证配置为 1 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 Firepower 1140 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 4 个情景的许可证。因此，聚合故障转移许可证包括 8 个情景。例如，一台设备可以使用 5 个情景，而另一台设备可以使用 3 个情景，例如；但在失败期间，一台设备将使用所有 8 个情景。由于一台设备的平台限制为 10，因此合并许可证最多允许 10 个情景；8 个情景在该限制范围内。
- 强加密 (3DES/AES) - 如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布

授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 1210/1220 的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1210 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 5 个情景的许可证。因此，聚合故障转移许可证包括 9 个情景。不过，由于一台设备的平台限制为 5，因此合并许可证最多仅允许 5 个情景。在此情况下，只能将主用情景许可证配置为 1 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1220 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 5 个情景的许可证。因此，聚合故障转移许可证包括 9 个情景。例如，一台设备可以使用 5 个情景，而另一台设备可以使用 4 个情景；但在故障期间，一台设备将使用全部 9 个情景。由于一台设备的平台限制为 10，因此合并许可证最多允许 10 个情景；9 个情景在该限制范围内。
- 强加密 (3DES/AES) - 如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使

用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能进行配置更改；否则操作不会受到影响。新主用设备每隔35秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 1230/1240/1250的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

故障转移功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1230 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 25 个情景的许可证。因此，聚合故障转移许可证包括 29 个情景。不过，由于一台设备的平台限制为 25，因此合并许可证最多仅允许 25 个情景。在此情况下，只能将主用情景许可证配置为 21 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1230 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 14 个情景。例如，一台设备可以使用 9 个情景，而另一台设备可以使用 5 个情景，例如；但在失败期间，一台设备将使用所有14个情景。由于一台设备的平台限制为 25，因此合并许可证最多允许 25 个情景；14 个情景在该限制范围内。
- 强加密 (3DES/AES) - 如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 3100 的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

故障转移功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 3130 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 100 个情景的许可证。因此，聚合故障转移许可证包括 104 个情景。不过，由于一台设备的平台限制为 100，因此合并许可证最多仅允许 100 个情景。在此情况下，只能将主用情景许可证配置为 95 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 3130 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 14 个情景。例如，一台设备可以使用 9 个情景，而另一台设备可以使用 5 个情景，例如；但在失败期间，一台设备将使用所有 14 个情景。由于一台设备的平台限制为 100，因此合并许可证最多允许 100 个情景；14 个情景在该限制范围内。

- 强加密 (3DES/AES) - 如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是 30 天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 4200 的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

故障转移功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 - 每台设备从服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 4215 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 250 个情景的许可证。因此，聚合故障转移许可证包括 254 个情景。不过，由于一台设备的平台限制为 250，因此合并许可证最多仅允许 250 个情景。在此情况下，只能将主用情景许可证配置为 246 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 4215 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 14 个情景。例如，一台设备可以使用 9 个情景，而另一台设备可以使用 5 个

情景，例如；但在失败期间，一台设备将使用所有14个情景。由于一台设备的平台限制为250，因此合并许可证最多允许 250 个情景；14 个情景在该限制范围内。

- 强加密 (3DES/AES) - 如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

适用于 Firepower 4100/9300 的故障转移许可证

智能软件管理器常规版和本地版

在配置故障转移之前，两个 Firepower 4100/9300 都必须向智能软件管理器或智能软件管理器本地服务器注册。辅助设备不会产生额外成本。

当您应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。使用令牌时，每个机箱必须具有相同的加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

为主用/备用故障转移启用故障转移后，只能在主用设备上配置用于主用/备用故障转移的 ASA 许可证配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。只有主用设备需要向服务器请求许可证。许可证将聚合为一个单独的故障转移许可证，供该故障转移对共享，并且此聚合许可证还将缓存在备用设备上，以便在该设备将来成为主用设备时使用。各个许可证类型将按以下方式进行管理：

- 基础—虽然只有主用设备需要向服务器请求此许可证，但默认情况下备用设备已启用了基础许可证；它不需要向服务器注册来使用它。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 10 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 10 个情景；对于 2 台设备，这些许可证相加之和为 20 个情景。您在主用/备用对中的主用设备上配置 250 个情景的许可证。因此，聚合故障转移许可证包括 270 个情景。不过，由于一台设备的平台限制为 250，因此合并许可证最多仅允许 250 个情景。在此情况下，只能将主用情景许可证配置为 230 个情景。

- 主用/主用： 基础 许可证包括 10 个情景；对于 2 台设备，这些许可证相加之和为 20 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 30 个情景。例如，一台设备可以使用 17 个情景，而另一台设备可以使用 13 个情景，例如；但在失败期间，一台设备将使用所有 30 个情景。由于一台设备的平台限制为 250，因此合并许可证最多允许 250 个情景；30 个情景在该限制范围内。

- 运营商 - 只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。
- 强加密 (3DES) - 如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能进行配置更改；否则操作不会受到影响。新主用设备每隔35秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 3100 的 ASA 群集许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，默认情况下，始终在所有设备上启用基础许可证。您只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 2 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 您在集群中有 6 个 Cisco Secure Firewall 3100。基础许可证包括 2 个情景；因为有 6 台设备，因此这些许可证加起来总共包括 12 个情景。您在控制设备上额外配置一个包含 20 个

情景的许可证。因此，聚合的集群许可证包括32个情景。由于一台机箱的平台限制为100，因此合并许可证最多允许 100 个情景；32 个情景在该限制范围内。因此，您可以在控制设备上配置最多 32 个情景；每台数据设备通过配置复制也将拥有 32 个情景。

- 您在集群中有 3 个 Cisco Secure Firewall 3100。基础许可证包括 2 个情景；因为有 3 台设备，因此这些许可证加起来总共包括 6 个情景。您在控制设备上额外配置一个包含 100 个情景的许可证。因此，聚合的集群许可证包括 106 个情景。由于一台设备的平台限制为 100，因此合并许可证最多允许 100 个情景；106 个情景超出限制范围。因此，您仅可以在控制设备上配置最多 100 个情景；每台数据设备通过配置复制也将拥有 100 个情景。在此情况下，只能将控制设备情景许可证配置为 94 个情景。

- 强加密 (3DES) - 如果您的智能账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账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新主用设备会每隔35秒发送一次权限授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

Cisco Secure Firewall 4200 的 ASA 群集许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，默认情况下，始终在所有设备上启用基础许可证。您只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。

- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 2 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 您在集群中有 6 个 Cisco Secure Firewall 4200。基础许可证包括 2 个情景；因为有 6 台设备，因此这些许可证加起来总共包括 12 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括32个情景。由于一台机箱的平台限制为250，因此合并许可证最多允许 250 个情景；32 个情景在该限制范围内。因此，您可以在控制设备上配置最多 32 个情景；每台数据设备通过配置复制也将拥有 32 个情景。
  - 您在集群中有 3 个 Cisco Secure Firewall 4200。基础许可证包括 2 个情景；因为有 3 台设备，因此这些许可证加起来总共包括 6 个情景。您在控制设备上额外配置一个包含 250 个情景的许可证。因此，聚合的群集许可证包括 256 个情景。由于一台设备的平台限制为 250，则聚合后的许可证最多允许 250 个情景；256 个情景超出了此限制。因此，您仅可以在控制设备上配置最多 250 个情景；每台数据设备通过配置复制也将拥有 250 个情景。在此情况下，只能将控制设备情景许可证配置为 244 个情景。
- 强加密 (3DES) - 如果您的智能账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账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新主用设备会每隔35秒发送一次权限授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

ASAv 的 ASA 集群许可证

智能软件管理器常规版和本地版

每台设备需要相同的吞吐量许可证和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集

群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 - 只有控制设备从服务器请求基础许可证，并且由于许可证汇聚，所有设备都可以使用标准许可证。
- 吞叶量 - 每台设备都会向服务器请求其自己的吞吐量许可证。
- 强加密 (3DES) - 如果您的智能账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账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每台设备单独购买许可证并启用。

Firepower 4100/9300 的 ASA 集群许可证

智能软件管理器常规版和本地版

集群功能本身不需要任何许可证。要使用强加密和其他可选许可证，每个 Firepower 4100/9300 机箱都必须注册到许可证颁发机构或智能软件管理器常规版和本地版中。数据设备不会产生额外成本。

当您应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。使用令牌时，每个机箱必须具有相同的加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 - 只有控制设备从服务器请求基础许可证，并且由于许可证汇聚，两个设备都可以使用标准许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 10 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 集群中有 6 个 Firepower 9300 模块。基础许可证包括 10 个情景；对于 6 台设备，这些许可证相加之和为 60 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括 80 个情景。由于一个模块的平台限制为 250，因此聚合后的许可证最多允许 250 个情景；80 个情景没有超出此限制。因此，您可以在控制设备上配置最多 80 个情景；每台数据设备通过配置复制也将拥有 80 个情景。
  - 集群中有 3 台 Firepower 4112 设备。基础许可证包括 10 个情景；对于 3 台设备，这些许可证相加之和为 30 个情景。您在控制设备上额外配置一个包含 250 个情景的许可证。因此，聚合的集群许可证包括 280 个情景。由于一台设备的平台限制为 250，则聚合后的许可证最多允许 250 个情景；280 个情景超出了此限制。因此，您仅可以在控制设备上配置最多 250 个情景；每台数据设备通过配置复制也将拥有 250 个情景。在此情况下，只能将控制设备情景许可证配置为 220 个情景。

- 运营商 - 分布式站点间 VPN 所需。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。
- 强加密 (3DES) - 对于 2.3.0 前 Cisco Software Manager 本地部署；或如果您的智能账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账户。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新的主用设备每12小时发送一次权利授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

智能软件许可的前提条件

智能软件管理器常规版和本地版前提条件

Firepower 4100/9300

在配置 ASA 许可授权之前，请在 Firepower 4100/9300 机箱上配置智能软件许可基础设施。

所有其他型号

- 确保来自设备的互联网访问、HTTP 代理访问或本地服务器访问上的智能软件管理器 。
- 配置 DNS 服务器，以使设备能够解析智能软件管理器的名称。
- 设置设备的时钟。
- 在思科智能软件管理器上创建账户：

  https://software.cisco.com/#module/SmartLicensing

  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账户。

永久许可证预留前提条件

- 在思科智能软件管理器上创建主账户：

  https://software.cisco.com/#module/SmartLicensing

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。即使ASA确实需要互联网连接到智能许可服务器以进行永久许可证预留，但智能软件管理器仍用于管理您的永久许可证。

- 获得许可团队的永久许可证预留支持。您必须提供使用永久许可证预留的正当理由。如果您的帐户未获得批准，则无法购买和应用永久许可证。
- 购买特殊的永久许可证（请参阅 每个型号的许可证 PID，第 83 页）。如果您的帐户中没有正确的许可证，则当您尝试在ASA上保留许可证时，将会看到类似于以下内容的错误消息：“许可证无法保留，因为虚拟帐户没有足够的剩余以下永久许可证：1-Firepower 4100 ASA PERM UNIV（永久）。“
- 永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅 Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。
- ASA Virtual： Azure 虚拟机监控程序不支持永久许可证预留。

智能软件许可准则

- 仅支持智能软件许可。对于 ASA Virtual上的较早软件，如果升级现有 PAK 许可的 ASA Virtual，则以前安装的激活密钥将被忽略，但会保留在设备上。如果将 ASA Virtual 降级，则将恢复激活密钥。
- 对于永久许可证预留，您必须在停用设备之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新设备。
- 由于思科传输网关使用具有不合规国家/地区代码的证书，因此在将 ASA 与该产品一起使用时，无法使用 HTTPS。您必须对思科传输网关使用 HTTP。

智能软件许可的默认设置

Smart Transport

默认情况下，所有设备型号都使用 Smart Transport 进行智能软件许可证通信，并使用以下 URL：

```
https://smartreceiver.cisco.com/licservice/license
```

对于 Firepower 4100/9300，必须在机箱级别启用智能软件许可证通信。

ASA Virtual

- 在部署 ASA Virtual时，您可设置功能层和吞吐量级别。此时仅 基础 级别可用。对于永久许可证预留，您不需要设置这些参数。当您启用永久许可证预留时，这些命令将从配置中删除。

注释 Essentials 许可证过去称为标准许可证，CLI 仍使用“标准”术语。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G | unlimited}
```

注释 如果您在 VMware 或 KVM 上使用的是 32 或 64 核心部署，则在 **throughput level** 命令中只能使用 **unlimited** 选项。

ASA Virtual: 配置智能软件许可

本节介绍如何为 ASA Virtual 配置智能软件许可。

ASA Virtual：配置常规智能软件许可

在部署 ASA Virtual 时，您可以预配置设备并包含一个注册令牌，以便其向智能软件管理器注册并启用智能软件许可。如果您需要更改 HTTP 代理服务器、许可证授权，或注册 ASA Virtual（例如，如果您未在 Day0 配置中包含 ID 令牌），请执行此任务。

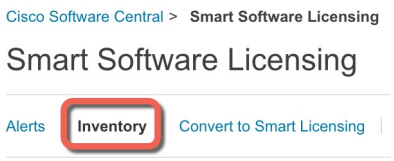
注释 您可能已经在部署您的 ASA Virtual时预配置了 HTTP 代理服务器和许可证授权。您还可能在部署 ASA Virtual时在 Day0 配置中包含了注册令牌；如果是这样，您就不需要使用此程序重新注册。

过程

步骤 1 （思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

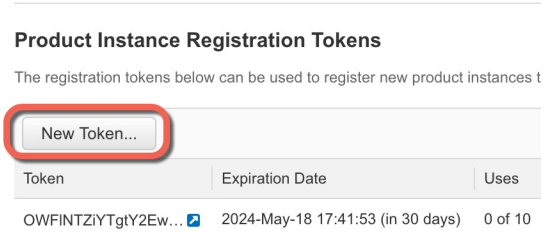
a) 点击**清单 (Inventory)**。

图 *1:* 清单



b) 在**常规 (General)** 选项卡上，点击**新建令牌 (New Token)**。

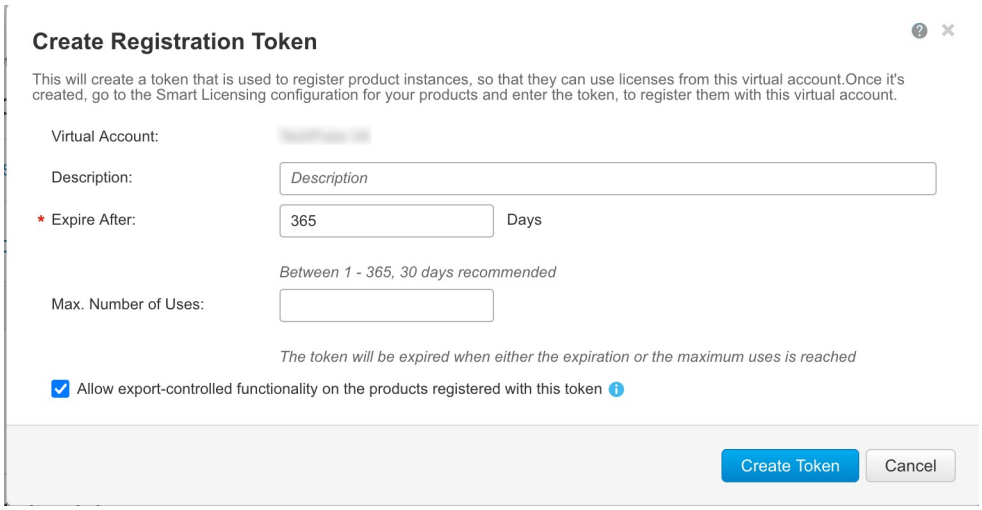
图 2: 新建令牌



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
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

图 3: 创建注册令牌



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 ASA 时，请准备好此令牌，以在该程序后面的部分使用。

图 *4:* 查看令牌

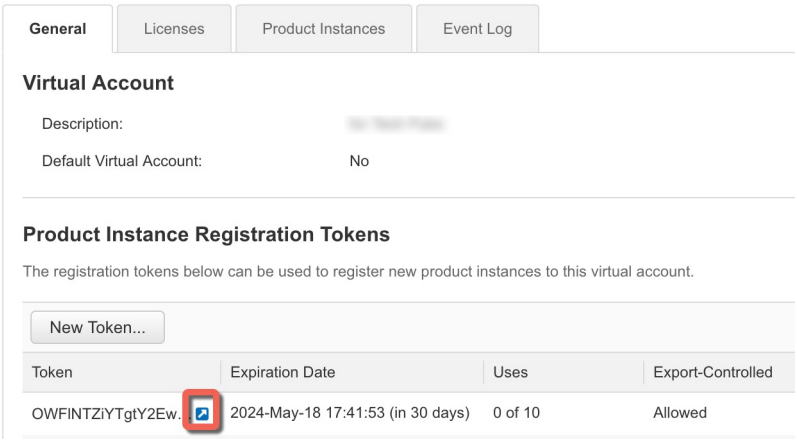
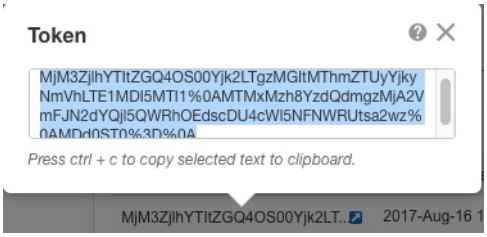


图 *5:* 复制令牌



步骤 2 （可选） 在 ASA Virtual 上，指定 Smart Transport 的 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不使用 Smart Transport，请参阅步骤 4 ，第 30 页。

注释

- 不支持认证的HTTP代理。
- 配置代理服务器 URL 时，请勿指定协议。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

步骤 3 配置许可证授权：

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。

c) 设置吞吐量级别，以便确定从智能软件管理器请求的许可证：

吞吐量级别 {**100M** | **1G** | **2G** | **10G** | **20G** | **无限制**}

注释
如果您使用的是 32 核或 64 核部署，则只有**无限制**选项可用。

请参阅以下吞吐量/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 - ASAvU

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （可选） 启用强加密。如果收到强加密令牌，**请不要** 输入此命令。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

注释
如果输入此命令，则设备将使用强加密许可证（无论是否需要）。因此，除非您的账户中具有该许可证，否则您的账户将不合规。由于使用强加密令牌时不需要此许可证，因此您可能会意外地使帐户不合规，并且没有任何好处。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

e) 退出许可证智能模式以应用更改：

exit

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**），或输入使您进入其他模式的任何命令。

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

步骤 4 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选） 指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

步骤 5 将 ASA Virtual 注册到智能软件管理器。

license smart register idtoken *id_token* [**force**]

ASA Virtual 尝试向智能软件管理器注册并请求对已配置的许可证授权进行授权。

注册 ASA Virtual时，智能软件管理器会为 ASA Virtual 和智能软件管理器之间的通信颁发 ID 证书。它还会将 ASA Virtual 分配到相应的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 ASA Virtual。

勾选 **强制** 关键词以注册已注册但可能与智能软件管理器不同步的 ASA Virtual 。例如，如果从智能软件管理器中意外删除了 ASA Virtual，请使用 **force**。

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

步骤 6 检查许可证状态。

show license status或**show running-config license**

如果与智能软件管理器的通信失败，请检查您是否配置了 DNS 服务器以及可访问服务器的正确路由。

示例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Supported
  VRF:
    Not Supported

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 27 2024 06:34:02 UTC
    Failure reason: {"token":["The token 'sgdgdsdg' is not valid."]}

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>
```

```
Miscellaneous:
  Custom Id: <empty>

Device Telemetry Report Summary:
================================
Data Channel: NOT AVAILABLE
Reports on disk: 0
```

示例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

ASA Virtual：为许可配置本地智能软件管理器

此程序适用于使用本地智能软件管理器的 ASA Virtual 。

开始之前

- 从 Cisco.com 下载智能软件管理器本地 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关更多信息，请参阅思科智能软件管理器本地部署产品手册。
- 在 7.0 版中，本地智能软件管理器中添加了 Smart Transport 。如果您使用的是旧版本，请按照此程序在 ASA Virtual 上启用 Smart Call Home。
- 在将设备置于气隙网络中之前，请下载加密 CA 信任池。该信任池通常会自动下载，但在气隙网络中可能会过期：

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

过程

步骤 1 在智能软件管理器本地上请求注册令牌。

步骤 2 （可选） 在 ASA Virtual 上，为 Smart Transport 指定 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不使用 Smart Transport，请参阅步骤 5 ，第 34 页。

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# license smart
```

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

步骤 3 更改许可证服务器 URL 以转到智能软件管理器本地。

license smart

transport url https://*on-Prem_ip_address***/SmartTransport**

要使用 Smart Call Home 而不使用 Smart Transport，请参阅步骤 5，第 34 页。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

步骤 4 配置许可证授权。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“**标准版**”。

c) 设置吞吐量级别，以便确定从智能软件管理器请求的许可证：

吞吐量级别 {**100M** | **1G** | **2G** | **10G** | **20G** | **无限制**}

注释
如果您使用的是 32 核或 64 核部署，则只有**无限制**选项可用。

请参阅以下吞吐量/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 - ASAvU

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （可选） 启用强加密。如果收到强加密令牌，**请不要** 输入此命令。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

注释
如果输入此命令，则设备将使用强加密许可证（无论是否需要）。因此，除非您的账户中具有该许可证，否则您的账户将不合规。由于使用强加密令牌时不需要此许可证，因此您可能会意外地使帐户不合规，并且没有任何好处。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

e) 退出许可证智能模式以应用更改：

exit

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**），或输入使您进入其他模式的任何命令。

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

步骤 5 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
```

```
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选）指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

c) 更改许可证服务器 URL 以转到智能软件管理器本地：

call-home

profile License

destination address http
https://*on-Prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

步骤 6 使用您在第 1 步中请求的令牌注册 ASA：

license smart register idtoken *id_token*

ASA 向本地智能软件管理器注册，并申请配置的许可证授权。如果您的帐户允许，则智能软件管理器本地还会应用强加密 (3DES/AES) 许可证。

注册 ASA Virtual时，智能软件管理器会为 ASA Virtual 和智能软件管理器本地部署之间的通信颁发 ID 证书。它还会将 ASA Virtual 分配到相应的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 ASA Virtual。

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

步骤 7 检查许可证状态。

show license status

如果与智能软件管理器的通信失败，请检查您是否配置了 DNS 服务器以及可访问服务器的正确路由。

示例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://10.1.5.5/SmartTransport
  Proxy:
    Not Supported
  VRF:
    Not Supported

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 27 2024 06:34:02 UTC
    Failure reason: {"token":["The token 'sgdgdsdg' is not valid."]}

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>

Device Telemetry Report Summary:
================================
Data Channel: NOT AVAILABLE
Reports on disk: 0
```

ASA Virtual：配置实用程序 (MSLA) 智能软件许可

通过托管服务许可协议 (MSLA) 的实用程序许可，您可以按许可证的使用时间来付费，而不是为许可证订用或永久许可证支付一次性费用。在实用程序许可模式下，ASA Virtual 会以时间为单位（15 分钟间隔）来跟踪许可证使用情况。ASA Virtual 智能代理每四个小时向智能软件管理器发送许可证使用情况报告（被称为 RUM 报告）。然后，使用情况报告将被转发到计费服务器。使用实用程序许可时，Smart Call Home 不会被用作许可消息的传输。消息将改为使用智能传输通过 HTTP/HTTPS 直接发送。

开始之前

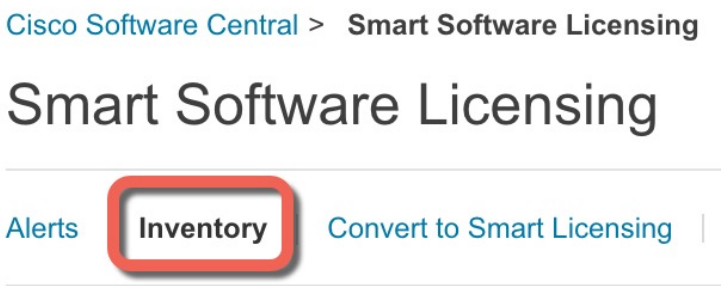
您可以使用本地智能软件管理器从 Cisco.com 下载智能软件管理器本地 OVA 文件，并在 VMware ESXi 服务器上安装和配置此文件。有关更多信息，请参阅思科智能软件管理器本地部署产品手册。

过程

步骤 1 在智能软件管理器（思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

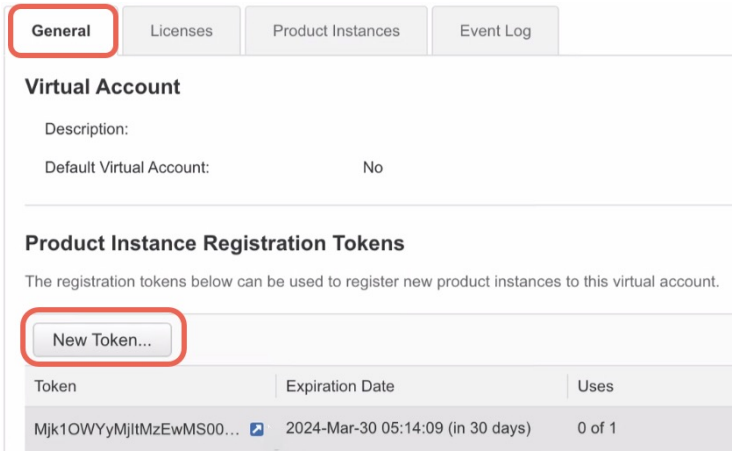
a) 点击**清单 (Inventory)**。

图 *6:* 清单



b) 在**常规 (General)** 选项卡上，点击**新建令牌 (New Token)**。

图 *7:* 新建令牌

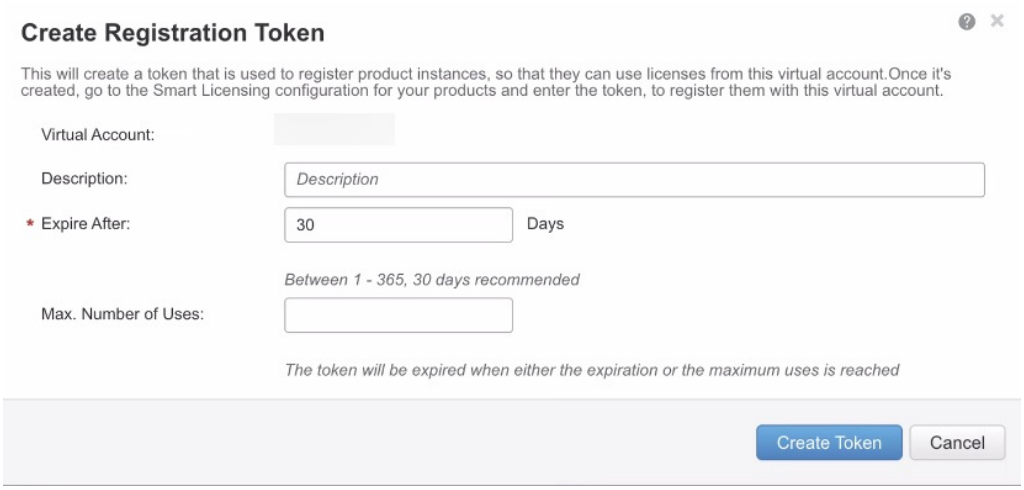


c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：

- **说明**
- **Expire After** - 思科建议该时间为 30 天。
- **最大值使用次数** - 令牌的最大使用次数。

令牌在到期日期或最大使用次数后到期。

图 *8:* 创建注册令牌



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 ASA 时，请准备好此令牌，以在该程序后面的部分使用。

图 *9:* 查看令牌

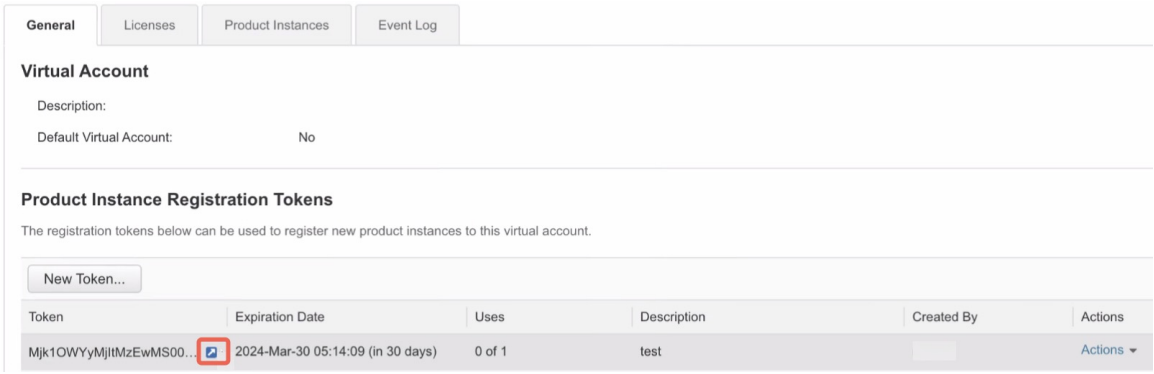
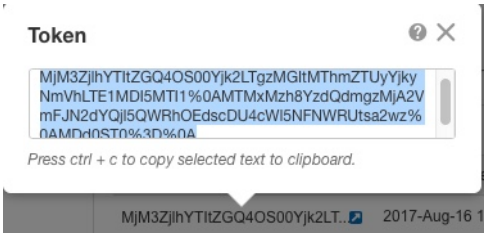


图 *10:* 复制令牌



步骤 2 在 ASA Virtual 上，配置智能许可参数。

a) 进入许可证智能配置模式。

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 启用智能传输。

transport type smart

实用程序许可需要使用 Smart Transport 而不是 Smart Call Home。

示例：

```
ciscoasa(config-smart-lic)# transport type smart
```

c) （可选） 指定智能软件管理器常规或本地部署的 URL。或者，您可以为许可证使用情况报告指定一个备选目标。

transport url {*transport_url* | **utility** *utility_url* | **default** }

如果未设置 URL，它将同时对智能传输和许可证使用情况报告使用 **default**，即 **https://smartreceiver.cisco.com/licservice/license**。

示例：

```
ciscoasa(config-smart-lic)# transport url http://server99.cisco.com/SmartTransport
ciscoasa(config-smart-lic)# transport url utility
http://server-utility.cisco.com/SmartTransport
```

d) （可选） 如果您的网络使用 HTTP 代理进行互联网访问，请配置代理地址。

transport proxy *proxy-url* **port** *proxy-port-number*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 443
```

e) 在许可消息中隐藏许可设备的主机名或智能代理版本号。

privacy {**all** | **hostname** | **version**}

示例：

```
ciscoasa(config-smart-lic)# privacy all
```

f) 设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“**标准版**”。

g) 设置吞吐量级别，以便确定从智能软件管理器请求的许可证：

吞吐量级别 {**100M** | **1G** | **2G** | **10G** | **20G** | **无限制**}

注释
如果您使用的是 32 核或 64 核部署，则只有**无限制**选项可用。

请参阅以下吞吐量/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 - ASAvU

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

h) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

i) 退出许可证智能模式以应用更改：

exit

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**），或输入使您进入其他模式的任何命令。

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

步骤 3 配置实用程序许可。

a) 进入实用程序配置模式。

utility

示例：

```
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)#
```

b) 创建唯一的客户标识符。此标识符包含在实用程序许可使用情况报告消息中。

custom-id *custom-identifier*

示例：

```
ciscoasa(config-smart-lic-util)# custom-id MyCustomID
```

c) 创建唯一的客户配置文件。此信息包含在实用程序许可使用情况报告中。

customer-info {**city** | **country** | **id** | **name** | **postalcode** | **state** |**street**} *value*

示例：

```
ciscoasa(config-smart-lic-util)# customer-info city MyCity
ciscoasa(config-smart-lic-util)# customer-info country MyCountry
ciscoasa(config-smart-lic-util)# customer-info id MyID
ciscoasa(config-smart-lic-util)# customer-info name MyName
ciscoasa(config-smart-lic-util)# customer-info postalcode MyPostalCode
ciscoasa(config-smart-lic-util)# customer-info state MyState
ciscoasa(config-smart-lic-util)# customer-info street MyStreet
```

d) 启用实用程序许可。

mode standard

示例：

```
ciscoasa(config-smart-lic-util)# mode standard
```

步骤 4 使用您在第 1 步中请求的令牌注册 ASA：

license smart register idtoken *id_token*

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

步骤 5 检查许可证状态。

show license status

如果与智能软件管理器的通信失败，请检查您是否配置了 DNS 服务器以及可访问服务器的正确路由。

示例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: ENABLED
  Utility report:
    Last success: May 14 2018 21:37:25 UTC
    Last attempt: SUCCEEDED on May 14 2018 21:37:24 UTC
    Next attempt: May 15 2018 01:37:24 UTC

  Customer Information:
    Id: MyID
    Name: MyName
    Street: MyStreet
    City: MyCity
    State: MyState
    Country: MyCountry
    Postal Code: MyPostalCode

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Smart
  Registration URL: http://server99.cisco.com/SmartTransport
  Utility URL: http://server-utility.cisco.com/SmartTransport

Registration:
  Status: REGISTERED
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on May 14 2018 21:37:20 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep 13 2018 13:34:40 UTC
  Registration Expires: May 14 2019 21:29:20 UTC

License Authorization:
  Status: AUTHORIZED on May 14 2018 21:37:22 UTC
  Last Communication Attempt: NOT STARTED
    Failure reason: Device in Thirdparty Utility Mode
  Next Communication Attempt: None
  Communication Deadline: Aug 12 2018 21:37:24 UTC
```

ASA Virtual：配置永久许可证预留

您可以为 ASA Virtual分配一个永久许可证。本部分介绍在您停用 ASA Virtual 时，或在更改模型层并且需要新的许可证时，如何退回许可证。

过程

步骤 1 安装 ASA Virtual 永久许可证，第 43 页

步骤 2 （可选）返还 ASA Virtual 永久许可证，第 47 页

安装 ASA Virtual 永久许可证

对于无法访问互联网的 ASA Virtual，您可以向智能软件管理器请求永久许可证。有关 ASA Virtual 永久许可证预留的详细信息，请参阅ASA Virtual 永久许可证预留，第 3 页。

注释

- 对于永久许可证预留，您必须在停用 ASA Virtual之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新的ASA Virtual。请参阅（可选）返还 ASA Virtual 永久许可证，第 47 页。
- 如果在安装永久许可证后清除配置（例如使用 **write erase**），则只需使用不带任何参数的 **license smart reservation** 命令重新启用永久许可证预留（如步骤 1 所示）；您不需要完成此程序的其余部分。

开始之前

- 购买永久许可证，以便其在智能软件管理器中可用。并非所有账户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得 Cisco 批准。
- 在 ASA Virtual 启动之后，您必须请求永久许可证；您不能在 第0天 配置期间安装永久许可证。

过程

步骤 1 （仅限 ASAv5，非灵活许可）当 DRAM 为 2GB（9.13 及更高版本中的最低要求）时，允许使用 ASAv5 永久许可证。

license smart set_plr5

步骤 2 （可选）运行该命令手动配置永久许可证预留，与 RAM 和 vCPU 无关（灵活的永久许可证预留模式）。

license smart flex-model {**asav5_plr** | **asav10_plr** | **asav30_plr** | **asav50_plr** | **asav100_plr** | **asavu_plr**}

注释
如果 ASA Virtual 的vCPU 超过 16 个，您只能配置 ASAvU（无限制）许可证。

要禁用灵活永久许可证预留，请在使用 **no license smart reservation** 命令禁用永久许可证预留模式后，使用此命令的 **no** 形式。

在灵活的永久许可证预留模式下，可以在启用许可证预留之前多次更改权限。如果要在启用许可证预留后更改权限，必须禁用永久许可证预留，用新的权限启用，然后再启用许可证预留。

例如，如果 ASA Virtual 具有 ASAv30 授权并且您已启用永久许可证预留：

```
asav1# license smart flex-model asav30_plr
asav1# license smart reservation
```

现在，如果将权限更改为 ASAv50，就会出现错误：

```
asav1# license smart flex-model asav50_plr
ERROR: Flexible PLR CLI is disabled when license reservation is enabled
```

要更改对 ASAv50 的授权，则必须执行以下操作：

```
asav1# no license smart reservation
asav1# license smart flex-model asav50_plr
asav1# license smart reservation
```

步骤 3 在 ASA Virtual CLI 中，启用永久许可证预留：

license smart reservation

示例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

要使用常规智能许可，请使用此命令的 **no** 形式。

步骤 4 请求要在智能软件管理器中输入的许可证代码：

license smart reservation request universal

示例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

为实现灵活许可：您可以更改分配给 ASA Virtual 的内存和 vCPU，而无需更改型号许可证。

对于非灵活许可：如果更改内存或vCPU，则必须退回当前许可证，并申请新型号级别的新许可证。请求的许可证必须与安装的内存和 vCPU 相匹配。有关 ASA Virtual 永久许可证预留的 vCPU 和内存到许可证矩阵的详细信息，请参阅ASA Virtual 永久许可证预留，第 3 页。

要更改已部署的 ASA Virtual的型号，在虚拟机监控程序中，可以更改 vCPU 和 DRAM 设置以匹配新的型号要求；有关这些值，参阅 ASA Virtual 快速入门指南。要查看您当前的型号，请使用 **show vm** 命令。

如果重新输入此命令，则会显示同一代码，即使在重新加载后也是如此。如果您尚未将此代码输入智能软件管理器，并且希望取消该请求，请输入：

license smart reservation cancel

如果禁用永久许可证预留，则所有待处理请求也会被取消。如果您已将该代码输入智能软件管理器，则必须完成此程序才能将该许可证应用于 ASA Virtual，然后可以根据需要退回该许可证。请参阅（可选）返还 ASA Virtual 永久许可证，第 47 页。

步骤 5 访问“智能软件管理器清单”(Smart Software Manager Inventory) 屏幕，点击**许可证 (Licenses)** 选项卡：

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

Licenses 选项卡显示与您的帐户相关的所有现有许可证（普通和永久）。

步骤 6 点击**许可证预留 (License Reservation)**，然后在**预留请求代码 (Reservation Request Code)** 字段中键入 ASA Virtual 代码。

步骤 7 点击**下一步**。

验证要**预留的许可证 (Licenses to Reserve)** 下面显示的永久许可证预留授权。该授权必须是您在步骤 2 中配置的授权。

步骤 8 点击**下一步 (Next)**。

步骤 9 查看信息，然后点击**生成授权码 (Generate Authorization Code)**。

智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

步骤 10 点击**关闭 (Close)**。

步骤 11 从 ASA Virtual CLI 中运行以下命令并输入授权码：

license smart reservation install *code*

示例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
INFO: ASAv platform license state is Licensed.
ciscoasa#
```

ASA Virtual 现在完全获得许可。

步骤 12 运行此命令可将运行配置保存到启动配置，避免在重启过程中丢失任何配置。

write memory

步骤 13 验证许可证状态和授权限制：

- **show license all**

```
asav1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
```

```
  Initial Registration: SUCCEEDED on Nov 12 2024 06:40:36 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 12 2024 06:27:23 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Supported
  VRF:
    Not Supported

Miscellaneous:
  Custom Id: <empty>

License Usage
=============

No licenses in use

Product Information
===================
UDI: PID:ASAv,SN:9A9PJLLB849

Agent Version
=============
Smart Agent for Licensing: 5.7.25_asav/5

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:ASAv,SN:9A9PJLLB849
      Reservation status: UNIVERSAL INSTALLED on Nov 12 2024 06:27:23 UTC
```

- **show license features**

```
asav1# show license features
Serial Number:  9AEJMLUP4D4
Export Compliant: YES

License mode: Smart Licensing
License reservation: Enabled
ASAv Platform License State: Licensed
Active entitlement: ASAv50_PLR, enforce mode: Authorized
Firewall throughput limited to 10 Gbps
Licensed features for this platform:
Maximum VLANs                     : 50
```

```
Inside Hosts                        : Unlimited
Failover                            : Active/Standby
Encryption-DES                      : Enabled
Encryption-3DES-AES                 : Enabled
Security Contexts                   : 0
Carrier                             : Enabled
AnyConnect Premium Peers            : 250
AnyConnect Essentials               : Disabled
Other VPN Peers                     : 250
Total VPN Peers                     : 250
AnyConnect for Mobile               : Enabled
AnyConnect for Cisco VPN Phone      : Enabled
Advanced Endpoint Assessment        : Enabled
Shared License                      : Disabled
Total TLS Proxy Sessions            : 500
Botnet Traffic Filter               : Enabled
Cluster                             : Enabled
```

（可选）返还 ASA Virtual 永久许可证

如果您不再需要永久许可证（例如，您要停用ASA Virtual或更改其型号级别使得它需要新许可证），必须使用此程序将该许可证正式返还给智能软件管理器。如果您不按照所有步骤操作，则该许可证仍将保持使用状态，并且无法轻松释放用于其他地方。

过程

步骤 1 从 ASA Virtual CLI 生成返还代码：

license smart reservation return

示例：

```
ciscoasa(config)# license smart reservation return
   WARNING: ASAv platform license state is Limited functionality.

   Enter this return code in Cisco Smart Software Manager portal:
   UDI: PID:ASAv,SN:9A6ST9AXQ24
       Return code: DrT1pZ-8cRT2N-xxxxx-64ABCD-xXYZeM-qD1
```

步骤 2 查看通用设备标识符 (UDI)，以便在智能软件管理器中找到此ASA Virtual实例：

步骤 3 访问智能软件管理器的“清单”(Inventory) 屏幕，然后点击**产品实例 (Product Instances)** 选项卡：

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

Product Instances 选项卡通过 UDI 显示所有获得许可的产品。

步骤 4 找到您想要取消许可的 ASA Virtual，依次选择**操作** > **删除**，然后在**预留退回码** 字段中键入 ASA Virtual。

永久许可证被返还到可用池。

步骤 5 点击**删除预留 (Remove Reservation)**。

步骤 6 要禁用永久许可证预留，请执行以下操作：

a) 要禁用永久许可证预留，请执行以下操作：

no license smart reservation

b) 禁用灵活的永久许可证预留，请执行以下操作：

no license smart flex-model {**asav5_plr** | **asav10_plr** | **asav30_plr** | **asav_50_plr** | **asav100_plr** | **asavu_plr**}

c) 使用以下命令确认许可证已取消注册：

show license features

命令输出显示 `No active entitlement`。

步骤 7 运行此命令可将运行配置保存到启动配置，避免在重启过程中丢失任何配置。

write memory

从非灵活 PLR 模式切换到灵活 PLR 模式

过程

步骤 1 从智能账户注销非灵活永久许可证预留许可证。

a) 从 ASA Virtual CLI 生成返还代码：

license smart reservation return

示例：

```
ciscoasa(config)# license smart reservation return
   WARNING: ASAv platform license state is Limited functionality.

   Enter this return code in Cisco Smart Software Manager portal:
   UDI: PID:ASAv,SN:9A6ST9AXQ24
       Return code: DrT1pZ-8cRT2N-xxxxx-64ABCD-xXYZeM-qD1
```

b) 查看通用设备标识符 (UDI)，以便在智能软件管理器中找到此 ASA Virtual实例：

c) 访问智能软件管理器的“清单”(Inventory) 屏幕，然后点击**产品实例 (Product Instances)** 选项卡：

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

Product Instances 选项卡通过 UDI 显示所有获得许可的产品。

d) 找到您想要使用 UDI 取消许可的 ASA Virtual 。

e) 找到您想要取消许可的 ASA Virtual，依次选择**操作** > **删除**，然后在**预留退回码** 字段中键入 。

f) 点击 **删除预留**

永久许可证被返还到可用池。

步骤 2 禁用永久许可证预留。ASA Virtual

a) 要禁用永久许可证预留，请执行以下操作：

no license smart reservation

步骤 3 用具有灵活永久许可证预留许可证注册ASA Virtual。有关详细信息，请参阅安装 ASA Virtual 永久许可证，第 43 页。

从灵活 PLR 模式切换到非灵活 PLR 模式

过程

步骤 1 从智能账户取消注册灵活永久许可证预留许可证。

a) 从 ASA Virtual CLI 生成返还代码：

license smart reservation return

示例：

```
ciscoasa(config)# license smart reservation return
   WARNING: ASAv platform license state is Limited functionality.

   Enter this return code in Cisco Smart Software Manager portal:
   UDI: PID:ASAv,SN:9A6ST9AXQ24
       Return code: DrT1pZ-8cRT2N-xxxxx-64ABCD-xXYZeM-qD1
```

b) 查看 ASA Virtual 通用设备标识符 (UDI)，以便在智能软件管理器中找到此 实例：

c) 访问智能软件管理器的“清单”(Inventory) 屏幕，然后点击**产品实例 (Product Instances)** 选项卡：

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

Product Instances 选项卡通过 UDI 显示所有获得许可的产品。

d) 找到您想要使用 UDI 取消许可的 ASA Virtual 。

e) 找到您想要取消许可的 ASA Virtual，依次选择**操作 (Actions)** > **删除 (Remove)**，然后在**预留退回码 (Reservation Return Code)** 字段中键入 。

f) 点击**删除预留**

永久许可证被返还到可用池。

步骤 2 禁用从ASA Virtual永久许可证预留。

a) 要禁用永久许可证预留，请执行以下操作：

no license smart reservation

b) 禁用灵活的永久许可证预留。

no license smart flex-model {**asav5_plr** | **asav10_plr** | **asav30_plr** | **asav_50_plr** | **asav100_plr** | **asavu_plr**}

步骤 3 向 ASA Virtual 注册具有非灵活永久许可证预留许可证的 。有关详细信息，请参阅安装 ASA Virtual 永久许可证，第 43 页。

（可选）取消注册 ASA Virtual（常规和本地）

对 ASA Virtual 取消注册会从帐户中删除 ASA Virtual。系统会删除 ASA Virtual 中的所有许可证授权和证书。您可能希望取消注册来为新的 ASA Virtual 释放许可证。或者，也可以从智能软件管理器删除 ASA Virtual。

注释 如果取消注册 ASA Virtual，则在重新加载 ASA Virtual后，它将恢复到严格的速率限制状态。

过程

取消注册 ASA Virtual：

license smart deregister

然后 ASA Virtual 会重新加载。

（可选）续约 ASA Virtual ID 证书或许可证授权 （常规和本地）

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，或者在智能软件管理器中进行了任何许可更改等操作，则可能要为这些项目手动续订注册。

过程

步骤 1 更新 ID 证书：

license smart renew id

步骤 2 更新许可证授权：

license smart renew auth

1000/1200/3100/4200：配置智能软件许可

本节介绍如何为 1000/1200/3100/4200 配置智能软件许可。选择以下方法之一：

- 1000/1200/3100/4200：配置常规智能软件许可，第 51 页

  您也可以（可选）取消注册 1000/1200/3100/4200（常规和本地），第 65 页或（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地），第 65 页。

- 1000/1200/3100/4200：配置智能软件本地许可，第 56 页

  您也可以（可选）取消注册 1000/1200/3100/4200（常规和本地），第 65 页或（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地），第 65 页。

- 1000/1200/3100/4200：配置永久许可证预留，第 61 页

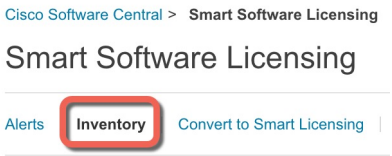
1000/1200/3100/4200：配置常规智能软件许可

此程序适用于使用智能软件管理器的 ASA。

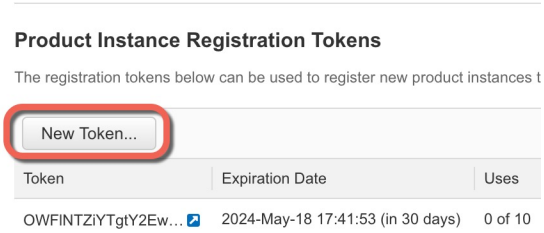
过程

步骤 1 在 Cisco Smart Software Manager 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

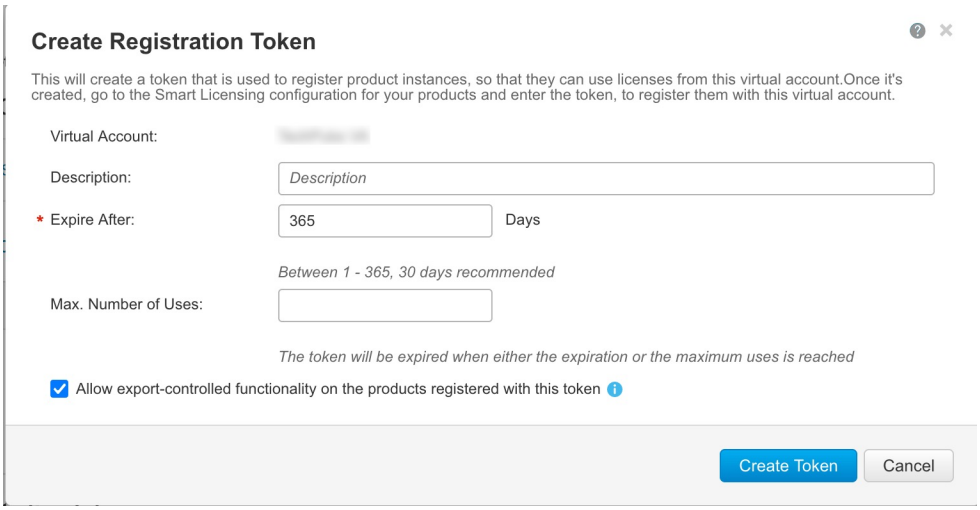
a) 点击**清单 (Inventory)**。



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
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

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ASA时，请准备好此令牌，以在该程序后面的部分使用。

图 *11:* 查看令牌

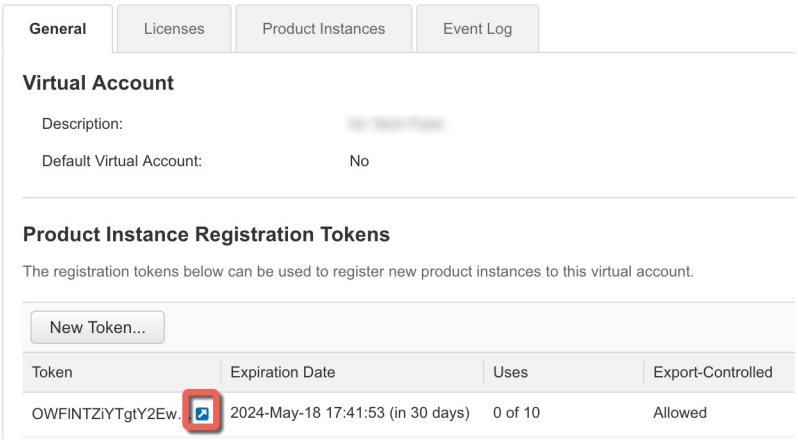
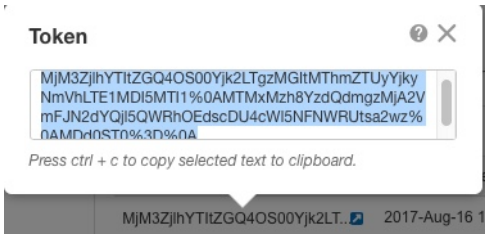


图 *12:* 复制令牌



步骤 2 （可选）

步骤 3 （可选） 在 ASA 上，为 Smart Transport 指定 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不是 Smart Transport，请参阅步骤步骤 5 ，第 55 页。

注释

- 不支持认证的HTTP代理。
- 配置代理服务器 URL 时，请勿指定协议。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

步骤 4 在 ASA 上请求许可证授权。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用；层许可证是添加其他功能许可证的前提条件。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。Cisco Secure Firewall 模型的 基础 许可证始终处于启用状态，无法禁用。

c) 请求安全情景许可证。

feature context 编号

注释
Firepower 1010 不支持此许可证。

默认情况下，ASA 支持 2 个情景，因此您应该请求的情景数量为需要的数量减去 2 个默认情景。情景的最大数量取决于您使用的型号：

- Firepower 1120 - 5 种情景
- Firepower 1140 - 10 种情景
- Firepower 1150 - 25 种情景
- Cisco Secure Firewall 1210 - 5 种情景
- Cisco Secure Firewall 1220 - 10 种情景
- Cisco Secure Firewall 1230 - 25 种情景
- Cisco Secure Firewall 1240 - 25 种情景
- Cisco Secure Firewall 1250 - 25 种情景
- Cisco Secure Firewall 3100 - 100 种情景
- Cisco Secure Firewall 4200 - 250 种情景

例如，对于 Firepower 1150 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

示例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （可选） (Firepower 1010) 请求增强型安全许可证以启用故障转移。

feature security-plus

示例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （可选） (Cisco Secure Firewall 3100/4200) 请求 Diameter、GTP/GPRS、SCTP 检测的运营商许可证。

feature carrier

示例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （可选） 启用强加密。如果收到强加密令牌，**请不要** 输入此命令。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

注释
如果输入此命令，则设备将使用强加密许可证（无论是否需要）。因此，除非您的账户中具有该许可证，否则您的账户将不合规。由于使用强加密令牌时不需要此许可证，因此您可能会意外地使帐户不合规，并且没有任何好处。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

步骤 5 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选） 指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

步骤 6 使用您在第 1 步中复制的令牌注册 ASA：

license smart register idtoken *id_token*

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA 向智能软件管理器注册，并申请配置的许可证授权。如果您的帐户允许，则智能软件管理器还会应用强加密 (3DES/AES) 许可证。使用 **show license summary** 或 **show running-config license** 命令检查许可证状态和使用情况。

示例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                     1 AUTHORIZED
```

示例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

1000/1200/3100/4200：配置智能软件本地许可

此程序适用于使用本地智能软件管理器的 ASA。

开始之前

- 从 Cisco.com 下载智能软件管理器本地 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关更多信息，请参阅思科智能软件管理器本地部署产品手册。

- 在 7.0 版中，本地智能软件管理器中添加了 Smart Transport 。如果您使用的是旧版本，请按照此程序在 ASA 上启用 Smart Call Home。
- 在将设备置于气隙网络中之前，请下载加密 CA 信任池。该信任池通常会自动下载，但在气隙网络中可能会过期：

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

过程

步骤 1 在智能软件管理器本地服务器上请求注册令牌。

步骤 2 （可选） 在 ASA 上，为 Smart Transport 指定 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不是 Smart Transport，请参阅步骤步骤 5 ，第 59 页。

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

步骤 3 更改许可证服务器 URL 以转到智能软件管理器本地。

license smart

transport url https://*on-Prem_ip_address***/SmartTransport**

要使用 Smart Call Home 而不是 Smart Transport，请参阅步骤步骤 5 ，第 59 页。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

步骤 4 在 ASA 上请求许可证授权。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用；层许可证是添加其他功能许可证的前提条件。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。Cisco Secure Firewall 模型的 基础 许可证始终处于启用状态，无法禁用。

c) （可选） 请求安全情景许可证。

feature context 编号

注释
Firepower 1010 和 Cisco Secure Firewall 1210/1220 不支持此许可证。

默认情况下，ASA 支持 2 个情景，因此您应该请求的情景数量为需要的数量减去 2 个默认情景。情景的最大数量取决于您使用的型号：

- Firepower 1120 - 5 种情景
- Firepower 1140 - 10 种情景
- Firepower 1150 - 25 种情景
- Cisco Secure Firewall 1210 - 5 种情景
- Cisco Secure Firewall 1220 - 10 种情景
- Cisco Secure Firewall 1230 - 25 种情景
- Cisco Secure Firewall 1240 - 25 种情景
- Cisco Secure Firewall 1250 - 25 种情景
- Cisco Secure Firewall 3100 - 100 种情景
- Cisco Secure Firewall 4200 - 250 种情景

例如，对于 Firepower 1150 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

示例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （可选） (Firepower 1010) 请求增强型安全许可证以启用故障转移。

feature security-plus

示例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （可选） (Cisco Secure Firewall 3100/4200) 请求 Diameter、GTP/GPRS、SCTP 检测的运营商许可证。

feature carrier

示例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （可选） 启用强加密。如果收到强加密令牌，**请不要** 输入此命令。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

注释
如果输入此命令，则设备将使用强加密许可证（无论是否需要）。因此，除非您的账户中具有该许可证，否则您的账户将不合规。由于使用强加密令牌时不需要此许可证，因此您可能会意外地使帐户不合规，并且没有任何好处。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

步骤 5 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选） 指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

c) 更改许可证服务器 URL 以转到智能软件管理器本地：

call-home

profile License

destination address http
https://*on-Prem_ip_address*/**Transportgateway/services/DeviceRequestHandler**

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

步骤 6 使用您在第 1 步中请求的令牌注册 ASA：

license smart register idtoken *id_token*

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA 向本地智能软件管理器服务器注册，并申请配置的许可证授权。如果您的帐户允许，则智能软件管理器还会应用强加密 (3DES/AES) 许可证。使用 **show license summary** 命令检查许可证状态和使用情况。

示例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
```

```
regid.2014-08.com.ci... (FP1010-ASA-Std)                    1 AUTHORIZED
```

1000/1200/3100/4200：配置永久许可证预留

您可以为 Firepower 1000, Cisco Secure Firewall 1200/3100/4200分配一个永久许可证。本节还介绍在停用 ASA 时如何退回许可证。

过程

步骤 1 安装 1000/1200/3100/4200 永久许可证，第 61 页。

步骤 2 （可选）返还 1000/1200/3100/4200 永久许可证，第 64 页。

安装 1000/1200/3100/4200 永久许可证

对于无法访问互联网 ASA，您可以向智能软件管理器请求永久许可证。永久许可证启用所有功能：具有最多安全情景的 基础 许可证。

注释 对于永久许可证预留，您必须在停用ASA之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新的ASA。请参阅（可选）返还 1000/1200/3100/4200 永久许可证，第 64 页。

开始之前

购买永久许可证，以便其在智能软件管理器中可用。并非所有账户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。

过程

步骤 1 在 ASA CLI 中，启用永久许可证预留：

license smart reservation

示例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

步骤 2 请求要在智能软件管理器中输入的许可证代码：

license smart reservation request universal

示例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

如果重新输入此命令，则会显示同一代码，即使在重新加载后也是如此。如果您尚未将此代码输入智能软件管理器，并且希望取消该请求，请输入：

license smart reservation cancel

如果禁用永久许可证预留，则所有待处理请求也会被取消。如果您已将该代码输入智能软件管理器，则必须完成此程序才能将该许可证应用于 ASA，然后可以根据需要退回该许可证。请参阅（可选）返还 1000/1200/3100/4200 永久许可证，第 64 页。

步骤 3 访问“智能软件管理器清单”(Smart Software Manager Inventory) 屏幕，点击**许可证 (Licenses)** 选项卡：

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

Licenses 选项卡显示与您的帐户相关的所有现有许可证（普通和永久）。

步骤 4 点击**许可证预留**，并在框中键入 ASA 代码。点击 **Reserve License**。

智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您没有看到 **License Reservation** 按钮，则您的帐户未被授权执行永久许可证预留。在这种情况下，您应禁用永久许可证预留并重新输入普通的智能许可证命令。

步骤 5 在 ASA 中输入授权码：

license smart reservation install *code*

示例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

步骤 6 在 ASA 上请求许可证授权。

注释
虽然永久许可证允许完全使用所有的许可证，但您仍需要打开 ASA 配置中的授权，以便 ASA 知道它可以使用它们。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
```

```
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用；层许可证是添加其他功能许可证的前提条件。基础版许可证以前称为标准版许可证，在CLI中仍称为“标准版”。Cisco Secure Firewall模型的 基础 许可证始终处于启用状态，无法禁用。

c) （可选） 启用安全情景许可证。

feature context 编号

注释
Firepower 1010 不支持此许可证。

默认情况下，ASA支持2个情景，因此您应该启用的情景数量为需要的数量减去2个默认情景。由于永久许可证允许最大数量，因此您可以为自己的型号启用最大数量。情景的最大数量取决于您使用的型号：

- Firepower 1120 - 5 种情景
- Firepower 1140 - 10 种情景
- Firepower 1150 - 25 种情景
- Cisco Secure Firewall 1210 - 5 种情景
- Cisco Secure Firewall 1220 - 10 种情景
- Cisco Secure Firewall 1230 - 25 种情景
- Cisco Secure Firewall 1240 - 25 种情景
- Cisco Secure Firewall 1250 - 25 种情景
- Cisco Secure Firewall 3100 - 100 种情景
- Cisco Secure Firewall 4200 - 100 种情景

例如，对于 Firepower 1150 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

示例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （可选） (Firepower 1010) 启用增强型安全许可证以启用故障转移。

feature security-plus

示例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （可选） (Cisco Secure Firewall 3100/4200) 启用 Diameter、GTP/GPRS、SCTP 检测的运营商许可证。

feature carrier

示例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （可选） 启用强加密。如果收到强加密令牌，**请不要** 输入此命令。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

注释
如果输入此命令，则设备将使用强加密许可证（无论是否需要）。因此，除非您的账户中具有该许可证，否则您的账户将不合规。由于使用强加密令牌时不需要此许可证，因此您可能会意外地使帐户不合规，并且没有任何好处。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

（可选）返还 1000/1200/3100/4200 永久许可证

如果不再需要永久许可证（例如，您正在停用 ASA），您必须使用以下程序将该许可证正式返还给智能软件管理器。如果您不按照所有步骤操作，则该许可证仍将保持使用状态，并且无法轻松释放用于其他地方。

过程

步骤 1 在 ASA 上生成返还代码：

license smart reservation return

示例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ASA 将立即变为未许可并进入“评估”状态。如果您需要再次查看此代码，请重新输入此命令。请注意，如果您请求新的永久许可证 (**license smart reservation request universal**)，则您无法重新显示此代码。确保捕获该代码以完成返还。如果评估期已过期，则ASA会进入过期状态。有关不合规状态的详细信息，请参阅 不合规状态，第 92 页。

步骤 2 查看 ASA 通用设备标识符 (UDI)，以便在智能软件管理器中找到此 ASA 实例：

show license udi

示例：

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

步骤 3 访问智能软件管理器的“清单”(Inventory) 屏幕，然后点击**产品实例 (Product Instances)** 选项卡：

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

Product Instances 选项卡通过 UDI 显示所有获得许可的产品。

步骤 4 找到您想要取消许可的ASA，依次选择**操作**>**删除**，然后在方框中键入ASA返还代码。点击**Remove Product Instance**。

永久许可证被返还到可用池。

（可选）取消注册 1000/1200/3100/4200（常规和本地）

取消注册 ASA 将从您的帐户删除 ASA。系统会删除 ASA 上的所有许可证授权和证书。您可能需要取消注册才能释放许可证以用于新的 ASA。或者，可以将 ASA 从智能软件管理器中删除。

过程

取消注册 ASA：

license smart deregister

（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地）

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 更新 ID 证书：

license smart renew id

步骤 2 更新许可证授权：

license smart renew auth

Firepower 4100/9300: 配置智能软件许可

此程序适用于使用智能软件管理器、本地智能软件管理器的机箱，或永久许可证预留；请参阅《FXOS配置指南》，以将你的方法配置为前提条件。您必须首先在ASA CLI中配置许可；请参阅FXOS配置指南以预配置许可证通信。

对于永久许可证预留，许可证可启用所有功能：具有最多安全情景和运营商许可证的标准层。但是，要让 ASA“知道”可以使用这些功能，您需要在 ASA 上启用它们。

开始之前

对于 ASA 集群，您需要访问控制单元进行配置。查看 Cisco Secure Firewall 机箱管理器 ，确定哪一台设备为控制单元。如该程序所示，您也可以从 ASA CLI 执行检查。

过程

步骤 1 连接到 Firepower 4100/9300 机箱 CLI（控制台或 SSH），然后将会话连接到 ASA：

connect module 插槽 **console connect asa**

示例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

下次连接到 ASA 控制台时，您会直接进入 ASA，不需要再次输入 **connect asa**。

对于 ASA 集群，您仅需要访问控制单元以进行许可证配置和其他配置。通常，控制单元位于插槽 1，因此，您首先应连接到该模块。

步骤 2 在 ASA CLI 中，进入全局配置模式。默认情况下，除非在部署逻辑设备时设置了启用密码，否则启用密码为空，但系统会在首次输入命令**enable**时提示您更改密码。

enable configure terminal

示例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa# configure terminal
asa(config)#
```

步骤 3 对于 ASA 集群，如果需要，请确认此设备是控制单元：

show cluster info

示例：

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

如果其他设备才是控制设备，请退出当前连接，并连接到正确的设备。有关如何退出连接，请参阅下文。

步骤 4 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

步骤 5 设置功能层：

feature tier standard

仅标准层可用。层许可证是添加其他功能许可证的前提条件。您的帐户中必须有足够的级别许可证。否则，无法配置任何其他功能许可证或需要许可证的任何功能。

步骤 6 请求以下功能中的一种或多种：

- 运营商 (GTP/GPRS、Diameter 和 SCTP 检测)

  feature carrier

- 安全情景

  feature context *<1-248>*

  对于永久许可证预留，您可以指定最大情景数 (248)。

- 强加密 (3DES/AES)

  feature strong-encryption

  如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账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账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

步骤 7 要退出 ASA 控制台，在提示符中输入输入 **~** 即可退出 Telnet 应用。输入 **quit** 以退回管理引擎 CLI。

每个型号的许可证

本部分列出可用于 ASAv 和 Firepower 4100/9300 机箱 ASA 安全模块的许可证授权。

ASA Virtual

使用 **throughput level** 命令在 ASA 配置中设置吞吐量水平时，对于灵活的永久许可证预留， 也可以使用 **license smart plr set** 命令指定型号，它将确定从智能软件管理器申请的许可证。请参阅以下吞吐量级别/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

- 无限制 — ASAvU

吞吐量级别还决定了最大 Secure Client 和 TLS 代理会话数。但是，较低的 ASA Virtual 内存配置文件将限制您的实际会话数，因此要确定您的会话，需要检查吞吐量级别和安装的内存。

ASA Virtual 的内存决定了最大并发防火墙连接数和 VLAN，而不是由吞吐量级别决定。

下表显示 ASA Virtual 系列已获许可的功能。

许可证	说明
许可证授权	
吞吐量级别	可以使用 **throughput level** 命令在 ASA 配置中设置吞吐量水平，对于灵活的永久许可证预留， 也可以使用 **license smart plr set** 命令指定型号。该级别会确定您需要的许可证。 100M: ASAv5 1G: ASAv10 2G: ASAv30 10G: ASAv50 20G: ASAv100 无限制：ASAvU
防火墙许可证	
僵尸网络流量过滤器	启用
防火墙连接数，并发	防火墙连接由 ASA Virtual 内存决定。 2 GB 至 7.9 GB：100,000 8 GB 至 15.9 GB：500,000 16 GB 至 31.9 GB：2,000,000 32 GB 至 64 GB：4,000,000 ASAvU：如果使用最小内存为 64 GB 的 ASAvU，则防火墙连接的最大数量为 8,000,000。
运营商	启用

许可证	说明
Total TLS Proxy Sessions	TLS 代理会话由吞吐量级别和 ASA Virtual 内存决定。 100M 吞吐量 + 任何内存：500 1G 吞吐量 + 任意内存：500 2G 吞吐量 • 2 GB 至 7.9 GB 内存：500 • 8 GB+ 内存：1000 10G 吞吐量 • 2 GB 至 7.9 GB 内存：500 • 8 GB 至 15.9 GB 内存：1000 • 16 GB 以上内存：10,000 20G 吞吐量 • 2 GB 至 7.9 GB 内存：500 • 8 GB 至 15.9 GB 内存：1000 • 16 GB 至 31.9 GB 内存：10,000 • 32 GB+ 内存：20,000 无限制吞吐量：如果您使用的是 ASAvU（最小内存为 64 GB），则 TLS 代理会话的最大数量为 40,000 个。
VPN 许可证	

许可证	说明	
Secure Client 对等体	未获得许可	Secure Client 对等体由吞吐量级别和 ASA Virtual 内存决定。 可选 *Secure Client Advantage* 或 *Secure Client Premier* 许可证，最多： *100M* 吞吐量 + 任何内存：*50* *1G* 吞吐量 + 任意内存：*250* *2G* 吞吐量 • *2 GB* 至 *7.9 GB* 内存：*250* • *8 GB*+ 内存：*750* *10G* 吞吐量 • *2 GB* 至 *7.9 GB* 内存：*250* • *8 GB* 至 *15.9 GB* 内存：*750* • *16 GB* 以上内存：*10,000* *20G* 吞吐量： • *2 GB* 至 *7.9 GB* 内存：*250* • *8 GB* 至 *15.9 GB* 内存：*750* • *16 GB* 至 *31.9 GB*：*10,000* • *32 GB*+ 内存：*20,000* 无限制吞吐量：如果您使用的是 ASAvU（其最小内存为 64 GB），则 Secure Client 对等体的最大数量为 40,000。

许可证	说明
其他 VPN 对等体	**注释** 其他 VPN 对等体由吞吐量级别和 ASA Virtual 内存决定。 100M 吞吐量 + 任何内存：50 1G 吞吐量 + 任意内存：250 2G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB+ 内存：750 10G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 以上内存：10,000 20G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 至 31.9 GB：10,000 • 32 GB+ 内存：20,000 无限制吞吐量：如果您使用的是ASAvU（其最小内存为64GB），则其他 VPN 对等体的最大数量为 40,000。

许可证	说明
VPN 对等体总数（包括所有类型）	注释 VPN 对等体总数由吞吐量级别和 ASA Virtual 内存决定。 100M 吞吐量 + 任何内存：50 1G 吞吐量 + 任意内存：250 2G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB+ 内存：750 10G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 以上内存：10,000 20G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 至 31.9 GB：10,000 • 32 GB+ 内存：20,000 无限制吞吐量：如果使用的是 ASAvU（它使用的最小内存为 64 GB），则最大 VPN 对等体数为 40,000。
通用许可证	
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置
故障转移	主用/备用
安全情景	不支持
集群	已启用
最大 VLAN 数量	VLAN 由 ASA Virtual 内存决定。 2 GB 至 7.9 GB - 50 8 GB 至 15.9 GB - 200 16 GB 至 31.9 GB - 1024 32 GB 至 64 GB - 1024

Firepower 1010

下表显示 Firepower 1010 已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	100,000	
运营商	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	4,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多：*75*
其他 VPN 对等体	75	
VPN 对等体总数（包括所有类型）	75	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
增强型安全（故障转移、VPN 负载均衡）	禁用	可选
安全情景	不支持。	
集群	不支持。	
最大 VLAN 数量	60	

Firepower 1100 系列

下表显示 Firepower 1100 系列已获许可的功能。

许可证	基础 许可证
防火墙许可证	

许可证	基础 许可证	
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Firepower 1120：200,000 Firepower 1140：400,000 Firepower 1150：600,000	
运营商	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	Firepower 1120：4,000 Firepower 1140：8,000 Firepower 1150：8,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Firepower 1120：150* *Firepower 1140：400* *Firepower 1150：800*
其他 VPN 对等体	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
VPN 对等体总数（包括所有类型）	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	2	可选许可证，最多： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*

许可证	基础 许可证
集群	不支持。
最大 VLAN 数量	1024

Cisco Secure Firewall 1210 和 1220

下表显示 Cisco Secure Firewall 1210 和 1220 系列已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Cisco Secure Firewall 1210：200,000 Cisco Secure Firewall 1220：300,000	
运营商	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	Cisco Secure Firewall 1210: 320 Cisco Secure Firewall 1220: 320	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 1210：200* *Cisco Secure Firewall 1220：300*
其他 VPN 对等体数	Cisco Secure Firewall 1210：200 Cisco Secure Firewall 1220：300	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 1210：200 Cisco Secure Firewall 1220：300	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	

许可证	基础 许可证	
安全情景	2	可选许可证，最多： *Cisco Secure Firewall 1210：5* *Cisco Secure Firewall 1220：10*
集群	不支持。	
最大 VLAN 数量	1024	

下表显示 Cisco Secure Firewall 1230、1240、1250 已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Cisco Secure Firewall 1230：400,000 Cisco Secure Firewall 1240：600,000 Cisco Secure Firewall 1250：1,000,000	
不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	Cisco Secure Firewall 1230：1000 Cisco Secure Firewall 1240：1000 Cisco Secure Firewall 1250：1000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 1230：500* *Cisco Secure Firewall 1240：1000* *Cisco Secure Firewall 1250：1500*
其他 VPN 对等体数	Cisco Secure Firewall 1230：500 Cisco Secure Firewall 1240：1000 Cisco Secure Firewall 1250：1500	

许可证	基础 许可证	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 1230：500 Cisco Secure Firewall 1240：1000 Cisco Secure Firewall 1250：1500	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	2	可选许可证，最多： *Cisco Secure Firewall 1230：25* *Cisco Secure Firewall 1240：25* *Cisco Secure Firewall 1250：25*
集群	启用	
最大 VLAN 数量	1024	

Cisco Secure Firewall 3100 系列

下表显示 Cisco Secure Firewall 3100 系列已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Cisco Secure Firewall 3105: 2,000,000 Cisco Secure Firewall 3110: 2,000,000 Cisco Secure Firewall 3120: 4,000,000 Cisco Secure Firewall 3130: 6,000,000 Cisco Secure Firewall 3140: 10,000,000	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	Cisco Secure Firewall 3105: 10,000 Cisco Secure Firewall 3110: 10,000 Cisco Secure Firewall 3120: 15,000 Cisco Secure Firewall 3130: 15,000 Cisco Secure Firewall 3140: 15,000	

许可证	基础 许可证	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 3105: 3000* *Cisco Secure Firewall 3110: 3000* *Cisco Secure Firewall 3120: 7000* *Cisco Secure Firewall 3130: 15,000* *Cisco Secure Firewall 3140: 20,000*
其他 VPN 对等体数	Cisco Secure Firewall 3105: 3000 Cisco Secure Firewall 3110: 3000 Cisco Secure Firewall 3120: 7000 Cisco Secure Firewall 3130: 15,000 Cisco Secure Firewall 3140: 20,000	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 3105: 3000 Cisco Secure Firewall 3110: 3000 Cisco Secure Firewall 3120: 7000 Cisco Secure Firewall 3130: 15,000 Cisco Secure Firewall 3140: 20,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	2	可选许可证，最多：*100*
集群	启用	
最大 VLAN 数量	1024	

Firepower 4100

下表显示 Firepower 4100 已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Firepower 4112：10,000,000 Firepower 4115：15,000,000 Firepower 4125：25,000,000 Firepower 4145：40,000,000	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	15,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*或 仅限 *Secure Client VPN* 许可证： *Firepower 4112: 10,000* *Firepower 4115: 15,000* *Firepower 4125: 20,000* *Firepower 4145: 20,000*
其他 VPN 对等体	Firepower 4112: 10,000 Firepower 4115: 15,000 Firepower 4125: 20,000 Firepower 4145: 20,000	
VPN 对等体总数（包括所有类型）	Firepower 4112: 10,000 Firepower 4115: 15,000 Firepower 4125: 20,000 Firepower 4145: 20,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	10	可选许可证：最多 *250*
集群	启用	
最大 VLAN 数量	1024	

Cisco Secure Firewall 4200 系列

下表显示 Cisco Secure Firewall 4200 系列已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Cisco Secure Firewall 4215：40,000,000 Cisco Secure Firewall 4225：90,000,000 Cisco Secure Firewall 4245：180,000,000	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	15,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 4215: 20,000* *Cisco Secure Firewall 4225: 25,000* *Cisco Secure Firewall 4245: 30,000*
其他 VPN 对等体数	Cisco Secure Firewall 4215: 20,000 Cisco Secure Firewall 4225: 25,000 Cisco Secure Firewall 4245: 30,000	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 4215: 20,000 Cisco Secure Firewall 4225: 25,000 Cisco Secure Firewall 4245: 30,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	10	可选许可证，最多：*250*
集群	启用	

许可证	基础 许可证
最大 VLAN 数量	1024

Firepower 9300

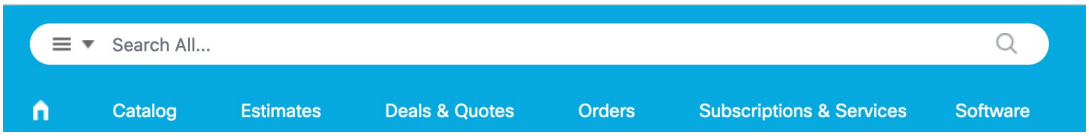
下表显示 Firepower 9300 已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Firepower 9300 SM-56: 60,000,000 Firepower 9300 SM-48: 60,000,000 Firepower 9300 SM-40: 55,000,000	
Carrier	禁用	可选许可证：运营商
TLS 代理会话总数	15,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证：最多 *20,000* 个
其他 VPN 对等体数	20,000	
VPN 对等体总数（包括所有类型）	20,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	10	可选许可证：最多 *250*
集群	启用	
最大 VLAN 数量	1024	

每个型号的许可证 PID

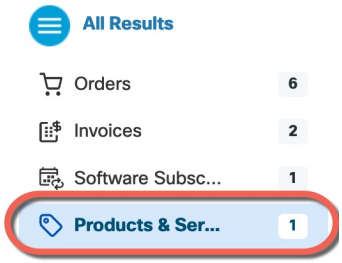
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的**搜索全部 (Search All)** 字段。

图 *13:* 许可证搜索



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

图 *14:* 结果



ASA Virtual PID

ASA Virtual 智能软件管理器常规版和本地版PID：

- ASAv5 许可证—L-ASAV5S-K9=
- ASAv10 许可证—L-ASAV10S-K9=
- ASAv30 许可证—L-ASAV30S-K9=
- ASAv50 许可证—L-ASAV50S-K9=
- ASAv100 许可证—L-ASAV100S-1Y=
- ASAv100 许可证—L-ASAV100S-3Y=
- ASAv100 许可证—L-ASAV100S-5Y=
- ASAvU 许可证—L-ASA-V-U-K9=

注释 ASAv 100 是基于预订的许可证，许可期限为 1 年、3 年或 5 年。

ASA Virtual 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。 Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

- ASAv5 许可证—L-ASAV5SR-K9=
- ASAv10 许可证—L-ASAV10SR-K9=
- ASAv30 许可证—L-ASAV30SR-K9=
- ASAv50 许可证—L-ASAV50SR-K9=
- ASAv100 许可证—L-ASAV100SR-K9=
- ASAvU 许可证—ASA-V-U-ULR-K9=

Firepower 1010 PID

Firepower 1010 智能软件管理器常规版和本地版 PID：

- 基础版 — L-FPR1000-ASA=。Required.
- 增强型安全 — L-FPR1010-SEC-PL=。增强型安全许可证启用了故障转移。
- 强加密 (3DES/AES)—L-FPR1K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 1010 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。 Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

- L-FPR1K-ASA-BPU=

Firepower 1100 PID

Firepower 1100 智能软件管理器常规版和本地版 PID：

- 基础版 — L-FPR1000-ASA=。Required.
- 5 情景 — L-FPR1K-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景 —L-FPR1K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 强加密 (3DES/AES)—L-FPR1K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 1100 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。 Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权

使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证， 第 9 页）。

- L-FPR1K-ASA-BPU=

Cisco Secure Firewall 1210/1220 PIDs

Secure Firepower 1210/1220 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 5 情景—CSF1200-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 强加密 (3DES/AES)—L-CSF1200-ENCK9=。仅当帐户未获授权使用强加密时需要。

Cisco Secure Firewall 1210/1220 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证， 第 9 页）。

- L-CSF1200-ASA-BPU=

Cisco Secure Firewall 1230/1240/1250 PID

Cisco Secure Firewall 1230/1240/1250 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 5 情景—CSF1200-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景—CSF1200-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 强加密 (3DES/AES)—L-CSF1200-ENCK9=。仅当帐户未获授权使用强加密时需要。

Cisco Secure Firewall 1230/1240/1250 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证， 第 9 页）。

- L-CSF1200-ASA-BPU=

Cisco Secure Firewall 3100 PID

Secure Firepower 3100 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 5 情景—L-FPR3K-ASASC-5=。情景许可证是累加的，可购买多个许可证。

- 10 情景—L-FPR3K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR3K-ASA-CAR=
- 强加密 (3DES/AES)—L-FPR3K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 3100 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 9 页）。

- L-FPR3K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 智能软件管理器常规版和本地版 PID：

- 基础版 — L-FPR4100-ASA=。Required.
- 10 情景 — L-FPR4K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 230 情景 — L-FPR4K-ASASC-230=。情景许可证是累加的，可购买多个许可证。
- 250 情景 — L-FPR4K-ASASC-250=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR4K-ASA-CAR=
- 强加密 (3DES/AES)—L-FPR4K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 4100 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 9 页）。

- L-FPR4K-ASA-BPU =

Cisco Secure Firewall 4200 PID

Secure Firepower 4200 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 5 情景—L-FPR4200-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景—L-FPR4200-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=
- 强加密 (3DES/AES)—L-FPR4200-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 4200 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

- L-FPR4200-ASA-BPU=

Firepower 9300 PID

Firepower 9300 智能软件管理器常规版和本地版 PID：

- 基础 - L-F9K-ASA =。Required.
- 10 情景 — L-F9K-ASA-SC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-F9K-ASA-CAR=
- 强加密 (3DES/AES)—L-F9K-ASA-ENCR-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 9300 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 9 页）。

- L-FPR9K-ASA-BPU =

监控智能软件许可

您可以监控许可证功能、状态和证书，以及启用调试消息。

查看您当前的许可证

如需查看许可证，请参阅以下命令：

- **show license features**

  以下示例显示 ASA 基础 许可证：

```
ciscoasa# show license features
Serial Number:  JAD254312UA
Export Compliant: YES

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 512
Inside Hosts                      : Unlimited
```

```
Failover                        : Active/Active
Encryption-DES                  : Enabled
Encryption-3DES-AES             : Enabled
Security Contexts               : 2
Carrier                         : Disabled
AnyConnect Premium Peers        : 150
AnyConnect Essentials           : Disabled
Other VPN Peers                 : 150
Total VPN Peers                 : 150
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Enabled
Advanced Endpoint Assessment    : Enabled
Shared License                  : Disabled
Total TLS Proxy Sessions        : 320
Cluster                         : Disabled
```

查看智能许可证状态

请参阅以下命令来查看许可证状态：

- **show license all**

  显示智能软件许可的状态、智能代理版本、UDI 信息、智能代理状态、全局合规性状态、授权状态、许可证书信息和排定的智能代理任务。

  以下示例显示 ASA Virtual 许可证：

```
ciscoasa# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
```

```
====================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
==============
Smart Agent for Licensing: 1.6_reservation/36
```

- **show license status**

  显示智能许可证状态。

  以下示例显示使用普通智能软件许可的 ASA Virtual 的状态：

```
ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

  以下 示例显示使用永久许可证预订的 ASA Virtual 的状态：

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC

Licensing HA configuration error:
    No Reservation Ha config error
```

- **show license summary**

  显示智能许可证状态和使用情况摘要。

  以下示例显示使用普通智能软件许可的 ASA Virtual 的摘要：

```
ciscoasa# show license summary
```

```
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (ASAv-STD-1G)                     1 AUTHORIZED
```

以下示例显示使用永久许可证预订的 ASA Virtual 的摘要：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  显示智能许可证使用情况。

  以下示例显示 ASA Virtual的使用情况：

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

查看 UDI

如需查看通用产品标识符 (UDI)，请参阅以下命令：

show license udi

以下示例显示 ASAv 的 UDI：

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

调试智能软件许可

请参阅以下用于调试集群的命令：

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  从智能代理打开调试。

- **debug license** *level*

  打开各种级别的智能软件许可管理器调试。

智能软件管理器通信

本部分介绍您的设备如何与智能软件管理器通信。

设备注册和令牌

对于每个虚拟账户，您可以创建注册令牌。默认情况下，此令牌有效期为30天。当部署每个设备或注册现有设备时，请输入此令牌 ID 以及授权级别。如果现有令牌已过期，则可以创建新的令牌。

注释 Firepower 4100/9300 机箱 - 设备注册是在机箱中而不是在 ASA 逻辑设备上进行配置。

在部署后或在现有设备上手动配置这些参数后启动时，设备会向智能软件管理器进行注册。使用令牌注册设备时，智能软件管理器会为设备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。

与智能软件管理器的定期通信

设备每30天与智能软件管理器通信一次。如果您在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。或者，也可以等待设备按计划通信。

您可以随意配置 HTTP 代理。

ASA Virtual

ASA Virtual 必须可以直接访问互联网，或者至少可每 90 天通过 HTTP 代理访问互联网。常规许可证通信每 30 天进行一次，但如果设备具有宽限期，则最多保持合规状态 90 天，而不会进行自动通报。宽限期后，您应该联系智能软件管理器，否则您的 ASA Virtual 将不合规；其他操作不受影响。

所有其他型号

ASA 必须可以直接访问互联网，或者至少每 90 天一次通过 HTTP 代理访问互联网。常规许可证通信每 30 天进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。在宽限期后，您必须联系智能软件管理器，否则您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。

不合规状态

设备在以下情况下可能会处于不合规状态：

- 过度使用 - 当设备使用不可用的许可证时。
- 许可证到期 - 当基于时间的许可证到期时。
- 通信不畅 - 当设备无法访问许可证颁发机构以重新获得授权时。

要验证您的帐户是否处于或接近不合规状态，必须将设备当前正在使用的授权与智能帐户中的授权进行比较。

根据具体型号，设备在不合规状态下可能受到限制：

- ASA Virtual- ASA Virtual 不受影响。
- 所有其他模型-您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。例如，基于 基础 许可证限制的现有环境可以继续运行，您可以修改它们的配置，但无法添加 新 环境。如果首次注册时没有足够的 基础 许可证，则无法配置任何许可功能，包括强加密功能。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件存在于用于指定智能软件管理器的 URL 的配置中。不能移除此配置文件。请注意，许可证配置文件的唯一可配置选项是智能软件管理器的目的地址 URL。除非获得 Cisco TAC 的指示，否则不应更改智能软件管理器 URL。

注释 对于 Firepower 4100/9300 机箱，用于许可的 Smart Call Home 在 Firepower 4100/9300 机箱管理引擎中，而不是 ASA 上进行配置。

不能为智能软件许可禁用 Smart Call Home。例如，即使使用 **no service call-home** 命令禁用 Smart Call Home，也不会禁用智能软件许可。

除非您专门配置其他 Smart Call Home 功能，否则不会开启这些功能。

智能许可证证书管理

ASA 会自动创建一个信任点，其中包含颁发 Smart Transport 或 Smart Call Home 服务器证书的 CA 的证书。为避免在服务器证书的颁发层次发生更改时出现服务中断，请配置 **auto-update** 命令以启用按照定期间隔自动更新信任池捆绑包。

从智能许可证服务器收到的服务器证书必须在 Extended Key Usage 字段中包括“ServAuth”。此检查仅在非自签名证书上完成；自签名证书在此字段中不提供任何值。

智能软件许可的历史记录

功能名称	平台版本	说明
增加了 Cisco Secure Firewall 4200 的连接限制	9.23(1)	已增加连接限制： • 4225: 80M → **90M** • 4245: 80M → **180M**
ASA Virtual 灵活永久许可证预留	9.23(1)	对于 ASA Virtual，您可以将任何特定型号的许可证配置为永久许可证预留，而与 RAM 和 vCPU 无关。 您的 ASA Virtual 内存 ASA Virtual 决定了最大安全客户端、TLS 代理会 Secure Client 话、最大并发防火墙连接和 VLAN。但是，较低的 ASA Virtual 内存配置文件将限制实际的会话和功能数量。 新增/修改的命令： **license smart flex-model**、**show license features**
为所有 Cisco Secure Firewall 1200 型号提供多情景支持	9.23(1)	我们增加了对 Cisco Secure Firewall 1210/1220 的多情景模式支持： • Cisco Secure Firewall 1210CE - 5 个情景。 • Cisco Secure Firewall 1210CP - 5 个情景。 • Cisco Secure Firewall 1220CX - 10 个情景。 多情景模式中不支持交换机端口，您必须先将所有接口转换为路由器接口，然后才能转换为多情景模式。 在其初始版本中，Cisco Secure Firewall 1230/1240/1250 还支持多情景模式： • Cisco Secure Firewall 1230- 25 个情景。 • Cisco Secure Firewall 1240- 25 个情景。 • Cisco Secure Firewall 1250- 25 个情景。

功能名称	平台版本	说明
Smart Transport 是与 CSSM 服务器通信的默认传输机制	9.22(1)	智能许可现在使用 Smart Transport 作为默认传输。如有必要，可以选择启用前一种类型 Smart Call Home 。 新增/修改的命令：**transport proxy**、**transport type**、**transport url**
ASAvU 许可证	9.22(1)	ASAvU 许可证在具有 32 核和 64 核的部署上实现最大吞吐量。此许可证仅在 VMware 和 KVM 上受支持。 新增/修改的命令：**throughput level unlimited**
增加了 Cisco Secure Firewall 4200 的连接限制	9.20(2)	已增加连接限制： • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
Cisco Secure Firewall 3100 支持运营商许可证	9.18(1)	运营商许可证启用 Diameter、GTP/GPRS、SCTP 检测。 新增/修改的命令：**feature carrier**
ASAv100 永久许可证预留	9.14(1.30)	ASAv100现在支持使用产品ID L-ASAV100SR-K9 =进行永久许可证预留。**请注意**：并非所有账户都被批准使用永久许可证预留。
ASA Virtual MSLA 支持	9.13(1)	ASA Virtual 支持思科托管服务许可协议（MSLA）程序，这是一种软件许可和消费体系，专为向第三方提供托管软件服务的思科客户和合作伙伴而设计。 MSLA 是一种新的智能许可形式，其中许可智能代理在时间单位内跟踪许可授权的使用情况。 新增/修改的命令：**license smart**、**mode**、**utility**、**custom-id**、**custom-info**、**privacy**、**transport type**、**transport url**、**transport proxy**
ASA Virtual 灵活许可	9.13(1)	灵活许可是智能许可的一种新形式，其中可以在受支持的 ASA Virtual vCPU/内存配置中使用任何 ASA Virtual 许可证。 Secure Client 和 TLS 代理的会话限制由安装的 ASA Virtual 平台授权确定，而不是与型号相关的平台限制。 新增/修改的命令：**show version**、**show vm**、**show cpu**、**show license features**
更改了 Firepower 4100/9300 机箱 上故障转移对的许可	9.7(1)	只有主用单元能够请求许可权利。过去，两种设备都需请求许可证授权。支持 FXOS 2.1.1。
适用于 ASA Virtual 短字符串增强的永久许可证预留	9.6(2)	由于智能代理的更新（更新至 1.6.4），请求和授权代码现在使用更短的字符串。 未修改任何命令。

功能名称	平台版本	说明
卫星服务器对 ASA Virtual的支持	9.6(2)	如果您的设备出于安全原因无法访问互联网，您可以选择以虚拟机 (VM) 形式安装本地智能软件管理器卫星服务器。 未修改任何命令。
适用于 Firepower 4100/9300 机箱 上 ASAv 的永久许可证预留	9.6(2)	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以为 Firepower 9300 和 Firepower 4100 上的 ASA 请求永久许可证。所有可用许可证授权均包括在永久许可证中，包括标准层、强加密（如果符合条件）、安全情景和运营商许可证。需要FXOS 2.0.1。 所有配置均在 Firepower 4100/9300 机箱 上执行；无需对 ASA 进行配置。
ASA Virtual 永久许可证预留	9.5(2.200) 9.6(2)	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以请求提供 ASA Virtual永久许可证。 在 9.6(2) 中，我们还为 Amazon Web 服务上的 ASA Virtual 添加了对此功能的支持。Microsoft Azure 不支持此功能。 引入了以下命令：**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return**
智能代理升级至 v1.6	9.5(2.200) 9.6(2)	智能代理从1.1版本升级到1.6版本。此升级支持永久许可证预留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。 **注释** 如果您从 9.5(2.200) 版本降级， ASA Virtual 将不保留许可注册状态。您需要在中，使用 **license smart register idtoken** *id_token* **force** 命令重新注册，并从智能软件管理器获取 ID 令牌。 引入了以下命令：**show license status**、**show license summary**、**show license udi**、**show license usage** 修改了以下命令：**show license all**、**show tech-support license** 弃用了以下命令：**show license cert**、**show license entitlement**、**show license pool**、**show license registration**

功能名称	平台版本	说明
强加密 (3DES) 许可证已自动应用于 Firepower 9300 上的 ASA	9.5(2.1)	对于一般的思科智能软件管理器用户，当他们在 Firepower 9300 上应用注册令牌时，只要符合相应条件，系统会自动启用强加密许可证。 **注释** 如果您通过智能软件管理器卫星部署使用 ASDM 和其他强加密功能，您必须在部署 ASA 之后使用 ASA CLI 启用强加密 (3DES) 许可证。 此功能要求具有 FXOS 1.1.3 版本。 删除了以下非卫星配置中的命令：**feature strong-encryption**
如果服务器证书的颁发层次结构出现更改，思科智能报障服务 (Smart Call Home)/智能许可 (Smart Licensing) 证书需进行验证	9.5(2)	智能许可使用 Smart Call Home 基础设施。当 ASA 首次在后台配置智能报障服务的匿名报告时，它会自动创建一个信任点，这个信任点包含颁发过智能报障服务证书的 CA 的证书。ASA 现在支持在服务器证书颁发层次结构出现变更时对证书进行验证；您可以按一定时间间隔定期启用 trustpool 捆绑的自动更新功能。 引入了以下命令：**auto-import**
新运营商许可证	9.5(2)	用于替换现有的 GTP/GPRS 许可证的新运营商许可证提供的支持包括 SCTP 和 Diameter 检测。对于 Firepower 9300 上的 ASA，**feature mobile-sp** 命令将自动迁移到 **feature carrier** 命令。 引入或修改了以下命令：**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version**
Firepower 9300 ASA 的思科智能软件许可	9.4(1.150)	我们为 Firepower 9300 ASA 引入了智能软件许可。 引入了以下命令：**feature strong-encryption, feature mobile-sp, feature context**
面向 ASA Virtual 的思科智能软件许可	9.3(2)	通过智能软件许可，您可以购买和管理许可证池。与 PAK 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASA Virtual，而不必管理每台设备的许可证密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。 引入了以下命令：**clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level**

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。