许可证：智能软件许可

通过思科智能软件许可，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 ASA 硬件型号和 ISA 3000 上不支持智能软件许可。它们使用 PAK 许可证。请参阅 关于 PAK 许可证。

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

本部分介绍智能软件许可的工作原理。

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，包括用于与许可证颁发机构进行通信的参数。Firepower 4100/9300 机箱本身无需任何许可证即可运行。

  注释 机箱间群集需要您在群集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，请单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账户。

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，也不能向许可证颁发机构注册，您可以配置离线许可。

永久许可证保留

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许可证颁发机构。与 PAK 许可证一样，您将为 ASA 购买一个许可证并安装许可证密钥。与PAK许可证不同的是，您将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。

ASAv 永久许可证预留

您可以获取特定于型号的，以启用所有功能：标准层；您的授权的最大吞吐量；强加密 (3DES/AES) 许可证（如果您的帐户符合条件）；和 AnyConnect 客户端功能已启用到平台的最大数量，具体取决于您购买的 AnyConnect 许可证是否有权使用 AnyConnect（请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- 100 Mbps 授权
- 1 Gbps 授权

- 2 Gbps 授权
- 10 Gbps 授权
- 20 Gbps 授权

您必须选择要在 ASAv 部署期间使用的授权级别。该授权级别会确定您请求的许可证。如果稍后要更改设备的授权级别，则必须退回当前许可证并在正确的授权级别请求新的许可证。要更改已部署的 ASAv 的型号，在虚拟机监控程序中，可以更改 vCPU 和 DRAM 设置以匹配新的授权要求；有关这些值，参阅 ASAv 快速入门指南。

如果您停止使用许可证，则必须通过在 ASAv 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。

Azure 虚拟机监控程序不支持永久许可证预留。

Firepower 1000 永久许可证预留

您可以获取启用所有功能的许可证：标准层；Security Plus (Firepower 1010)；最大安全情景数量 (Firepower 1100)；强加密 (3DES/AES) 许可证（如果您的帐户符合条件）；以及， AnyConnect 客户端功能已启用到平台的最大数量，具体取决于您购买的 AnyConnect 许可证是否支持使用 AnyConnect 的权限（请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

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 2100 永久许可证预留

您可以获取启用所有功能的许可证：标准层；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）；以及 AnyConnect 客户端功能已启用到平台的最大数量，具体取决于您购买的 AnyConnect 许可证是否启用使用 AnyConnect 的权利（请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。您还需要在 ASA 配置中请求授权，以便 ASA 允许其使用。

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

您可以获取启用所有功能的许可证：标准层；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）；以及 AnyConnect 客户端功能已启用到平台的最大数量，具体取决于您购买的 AnyConnect 许可证是否具有使用 AnyConnect 的权利（请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。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。

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。

卫星服务器（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（也称为本地部署）服务器。该卫星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。只有卫星需要定期连接到主许可证颁发机构以同步您的许可证使用。您可以按时间表执行同步，也可以手动同步。

卫星服务器上可以执行以下功能：

- 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

有关详细信息，请参阅《智能软件管理器卫星》。

按虚拟账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

ASAv

ASAv 不支持评估模式。在 ASAv 向许可证颁发机构注册之前，它会在严格限制速率的状态下运行。

Firepower 1000

在 Firepower 1000 向许可证颁发机构注册之前，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，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)；您必须向许可证颁发机构注册，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 向许可证颁发机构注册之前，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，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)；您必须向许可证颁发机构注册，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 机箱向许可证颁发机构注册之前，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 机箱向许可证颁发机构注册之后，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)；您必须向许可证颁发机构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。

AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证

AnyConnect Plus、AnyConnect Apex 或仅 VPN 许可证是可应用于多个 ASA 的多用途许可证，所有这些 ASA 都共享许可证指定的一个用户池。使用智能许可的设备不需要对实际平台实际应用任何 AnyConnect 许可证。但仍必须购买相同的许可证，并且仍必须将合同编号关联至您的 Cisco.com ID，以获取软件中心访问权和技术支持。有关详情，请参阅：

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

其他 VPN 许可证

其他 VPN 会话包括以下 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。

组合所有类型的 VPN 会话总数

- 虽然最大总 VPN 会话数累计超过最大 VPN AnyConnect 会话数和其他 VPN 会话数，但是合并会话数不应超过 VPN 会话限制。如果超出了最大 VPN 会话数，可以对 ASA 实施过载，以确保相应地调整网络大小。

- 如果启动无客户端 SSL VPN 会话，然后从门户启动 AnyConnect 客户端会话，则总共会使用 1 个会话。但是，如果先启动 AnyConnect 客户端（例如，通过独立客户端），然后登录无客户端 SSL VPN 门户，则会使用 2 个会话。

加密许可证

强加密：ASAv

强加密 (3DES/AES) 可在您连接到许可证颁发机构或卫生服务器之前用于管理连接，以便您能够启动 ASDM 并连接到许可证颁发机构。对于通过设备的流量，在您连接到许可证颁发机构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 ASAv 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 ASAv 之后变为不合规状态，只要已成功应用导出合规性令牌，ASAv 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 ASAv，并且禁用了导出合规性，或者如果您将 ASAv 还原到出厂默认设置，系统将会删除该许可证。

如果您最初注册的 ASAv 没有强加密，后来又添加了强加密，则必须重新加载 ASAv 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。

对于 2.3.0 版以前的卫星服务器版本，您必须在 ASA 配置中手动请求强加密许可证（不支持导出合规性令牌）；这种情况下，如果 ASAv 变为不合规状态，吞吐量将会严重受限。

强加密：设备模式下的 Firepower 1000 和 Firepower 2100

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到许可证颁发机构，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许可证，这要求您先向许可证颁发机构注册。

注释 如果您在拥有许可证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。

对于 2.3.0 版以前的卫星服务器版本，您必须在 ASA 配置中手动请求强加密许可证（不支持导出合规性令牌）；这种情况下，如果 ASA 变为不合规状态，将不允许通过流量。

强加密：平台模式下的 Firepower 2100

强加密 (3DES/AES) 可在您连接到许可证颁发机构或卫星服务器之前用于管理连接，以便您能够启动 ASDM。请注意，ASDM 访问仅在具有默认加密的管理专用接口上可用。在您连接并获取强加密许可证之前，不允许通过设备的流量。

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。

对于 2.3.0 版以前的卫星服务器版本，您必须在 ASA 配置中手动请求强加密许可证（不支持导出合规性令牌）；这种情况下，如果 ASA 变为不合规状态，将不允许通过流量。

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，不允许通过设备的流量。

当您向智能软件许可帐户请求Firepower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。

对于不支持导出合规性令牌的 2.3.0 版以前的卫星服务器版本：您必须使用 CLI 手动请求 ASA 配置中的强加密许可证，因为 ASDM 需要 3DES。如果 ASA 变为不合规状态，则不允许需要此许可证的管理流量和通过流量。

DES：所有型号

无法禁用 DES 许可证。如果您安装有 3DES 许可证，则 DES 仍然可用。要在希望仅使用强加密时防止使用 DES，请务必将所有相关命令都配置为仅使用强加密。

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
- GTP/GPRS
- SCTP

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）。如果使用故障切换并输入 **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。

故障切换或 ASA 集群许可证

ASAv 的故障切换许可证

备用设备需要与主设备相同型号的许可证。

Firepower 1010 的故障切换许可证

常规或卫星智能许可

两个 Firepower 1010 单元都必须向许可证颁发机构或卫星服务器注册。两台设备都要求您先启用标准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。

如果需要在 ASA 中启用强加密(3DES/AES)功能许可证（例如，对于预2.3.0 版以前思科智能软件管理器卫星部署或跟踪访客访问），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切换许可证，供该故障切换对共享，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。在故障切换后，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。故障切换对使用聚合许可证的期限是30天，如果该故障切换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。如果解散该故障切换对，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，必须在配置故障切换之前为每台机箱单独购买许可证并启用。

Firepower 1100 的故障切换许可证

常规或卫星智能许可

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

为主用/备用故障切换启用故障切换后，只能在主用设备上配置智能许可。对于主用/主用故障切换，只能在故障切换组 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 在形成故障切换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，在使用具有故障切换功能的强加密令牌时，您有两种许可选择：

- 在启用故障切换之前，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，在启用故障切换后，继续在主用设备上配置许可证授权。如果为故障切换链路启用加密，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，请启用故障切换。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，如果您在故障切换链路上启用了加密，系统将使用 DES（弱加密），因为故障切换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：

- 标准 - 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标准许可证；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，默认情况下标准许可证包括 2 个情景，并存在于两台设备上。每台设备的标准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：
  - 标准许可证包括 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，聚合故障切换许可证包括 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。
  - 标准许可证包括 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，聚合故障切换许可证包括 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，总共 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)（适用于 2.3.0 版以前的思科智能软件管理器卫星部署，当无法使用强加密令牌或用于跟踪目的）— 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。

在故障切换后，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。故障切换对使用聚合许可证的期限是30天，如果该故障切换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。如果解散该故障切换对，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，必须在配置故障切换之前为每台机箱单独购买许可证并启用。

Firepower 2100 的故障切换许可证

常规或卫星智能许可

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

为主用/备用故障切换启用故障切换后，只能在主用设备上配置智能许可。对于主用/主用故障切换，只能在故障切换组 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 在形成故障切换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，在使用具有故障切换功能的强加密令牌时，您有两种许可选择：

- 在启用故障切换之前，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，在启用故障切换后，继续在主用设备上配置许可证授权。如果为故障切换链路启用加密，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，请启用故障切换。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，如果您在故障切换链路上启用了加密，系统将使用 DES（弱加密），因为故障切换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：

- 标准 - 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标准许可证；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，默认情况下标准许可证包括 2 个情景，并存在于两台设备上。每台设备的标准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：
  - 标准许可证包括 2 个情景；对于两个 FirePower 2130 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 30 个情景的许可证。因此，聚合故障切换许可证包

括 34 个情景。不过，由于一台设备的平台限制为 30，因此合并许可证最多仅允许 30 个情景。在此情况下，只能将主用情景许可证配置为 25 个情景。

- 标准许可证包括 2 个情景；对于两个 FirePower 2130 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，聚合故障切换许可证包括 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，总共 14 个情景。由于一台设备的平台限制为 30，因此合并许可证最多允许 30 个情景；14 个情景在该限制范围内。

- 强加密 (3DES/AES)（适用于 2.3.0 版以前的思科智能软件管理器卫星部署，当无法使用强加密令牌或用于跟踪目的）— 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。

在故障切换后，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。故障切换对使用聚合许可证的期限是 30 天，如果该故障切换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。如果解散该故障切换对，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，必须在配置故障切换之前为每台机箱单独购买许可证并启用。

Firepower 4100/9300 机箱上适用于 ASA 的故障切换许可证

常规或卫星智能许可

两个 Firepower 4100/9300 机箱 都必须注册到许可证颁发机构或卫星服务器中。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/备用故障切换启用故障切换后，只能在主用设备上配置用于主用/备用故障切换的 ASA 许可证配置智能许可。对于主用/主用故障切换，只能在故障切换组 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切换许可证，供该故障切换对共享，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：

- 标准 - 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标准许可证；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，默认情况下标准许可证包括 10 个情景，并存在于两台设备上。每台设备的标准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：

- 标准许可证包括 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，聚合故障切换许可证包括 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。
- 标准许可证包括 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，聚合故障切换许可证包括 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，总共 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)（适用于 2.3.0 版以前的思科智能软件管理器卫星部署，当无法使用强加密令牌或用于跟踪目的）— 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。

在故障切换后，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。故障切换对使用聚合许可证的期限是 30 天，如果该故障切换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。如果解散该故障切换对，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，必须在配置故障切换之前为每台机箱单独购买许可证并启用。

Firepower 4100/9300 的 ASA 群集许可证

常规或卫星智能许可

群集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卫星服务器中。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群集设备共享的群集许可证，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：

- 标准：只有控制设备从服务器请求标准许可证，并且由于许可证聚合，两台设备都可以使用该许可证。

- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，标准许可证包括 10 个情景，并且位于所有群集成员上。每台设备的标准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群集许可证中的平台限制。例如：
  - 群集中有 6 个 Firepower 9300 模块。标准许可证包括 10 个情景；因为有 6 台设备，因此这些许可证加起来总共包括 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，聚合的群集许可证包括 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。
  - 群集中有 3 台 Firepower 4110 设备。标准许可证包括 10 个情景；因为有 3 台设备，因此这些许可证加起来总共包括 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，聚合的群集许可证包括 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)（适用于 2.3.0 以前版本的思科智能软件管理器卫星部署，或适用于跟踪访客访问），此许可证按设备进行授权，每台设备从服务器请求自己的许可证。

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群集后，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。如果某台设备退出群集，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，您需要在非群集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，必须在配置群集之前为每个机箱单独购买许可证并启用。

智能软件许可必备条件

常规和卫星智能许可证必备条件

ASAv，Firepower 1000，Firepower 2100

- 确保来自设备的互联网访问、HTTP 代理访问或卫星服务器访问。
- 配置 DNS 服务器，以使设备能够解析许可证颁发机构的名称。
- 设置设备的时钟。在设备模式下的 Firepower 2100, 上，您在 FXOS 中设置时钟。

- 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，请单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账户。

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。

永久许可证预留必备条件

- 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，请单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账户。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（请参阅许可证PID，第15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）。“

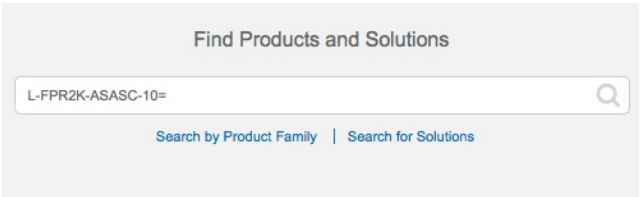
- 永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。AnyConnect 客户端功能也会根据平台购买的最大数量启用，具体取决于您购买的 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- ASAv： Azure 虚拟机监控程序 不支持永久许可证预留。

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 **Find Products and Solutions** 搜索字段。搜索以下许可证产品 ID (PID)。

图 *1:* 许可证搜索



ASAv PID

ASAv 常规和卫星智能许可 PID：

- ASAv5—L-ASAV5S-K9=
- ASAv10—L-ASAV10S-K9=
- ASAv30—L-ASAV30S-K9=
- ASAv50—L-ASAV50S-K9=
- ASAv100—L-ASAV100S-1Y=
- ASAv100-L-ASAV100S-3Y =
- ASAv100—L-ASAV100S-5Y=

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。

ASAv 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）。AnyConnect 客户端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 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- ASAv5—L-ASAV5SR-K9=
- ASAv10-L-ASAV10SR-K9 =
- ASAv30—L-ASAV30SR-K9=
- ASAv50—L-ASAV50SR-K9=
- ASAv100—L-ASAV100SR-K9=

Firepower 1010 PID

Firepower 1010 常规和卫星智能许可PID：

- 标准许可证 - L-FPR1000-ASA =。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 增强型安全许可证-L FPR1010-SEC-PL =。增强型安全许可证启用了故障转移。
- 强加密 (3DES/AES) 许可证 - L-FPR1K-ENC-K9=。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。

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）。AnyConnect 客户端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 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- L-FPR1K-ASA-BPU =

Firepower 1100 PID

Firepower 1100 常规和卫星智能许可 PID：

- 标准许可证 - L-FPR1000-ASA =。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 5 情景许可证 - L-FPR1K-ASASC-5=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 10 情景许可证 - L-FPR1K-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 强加密 (3DES/AES) 许可证 - L-FPR1K-ENC-K9=。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。

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）。AnyConnect 客户端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 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- L-FPR1K-ASA-BPU=

Firepower 2100 PID

Firepower 2100 常规和卫星智能许可 PID：

- 标准许可证 - L-FPR2100-ASA=。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 5 情景许可证 - L-FPR2K-ASASC-5=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 10 情景许可证 - L-FPR2K-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 强加密 (3DES/AES) 许可证 - L-FPR2K-ENC-K9=。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。

Firepower 2100 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）。AnyConnect 客户端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 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- L-FPR2K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 常规和卫星智能许可 PID：

- 标准许可证 - L-FPR4100-ASA =。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 10 情景许可证 - L-FPR4K-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 230 情景许可证 - L-FPR4K-ASASC-230=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 250 情景许可证 - L-FPR4K-ASASC-250=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 运营商（Diameter、GTP/GPRS、SCTP）- L-FPR4K-ASA-CAR=
- 强加密 (3DES/AES) 许可证 - FPR4K-ENC-K9 =。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。

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）。AnyConnect 客户端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 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- L-FPR4K-ASA-BPU =

Firepower 9300 PID

Firepower 9300 常规和卫星智能许可 PID：

- 标准许可证 - L-F9K-ASA =。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 10 情景许可证 - L-F9K-ASA-SC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 运营商（Diameter、GTP/GPRS、SCTP）- L-F9K-ASA-CAR=

- 强加密 (3DES/AES) 许可证 - L-F9K-ASA-ENCR-K9=。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。

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）。AnyConnect 客户端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 AnyConnect 许可证是否具有权使用 AnyConnect （请参阅 AnyConnect Plus、AnyConnect Apex 和仅 VPN 许可证，第 5 页）。

- L-FPR9K-ASA-BPU =

智能软件许可指南

- 仅支持智能软件许可。对于 ASAv 上的较早软件，如果升级现有 PAK 许可的 ASAv，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 ASAv 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

ASAv

- ASAv 默认配置包括名为“License”的 Smart Call Home 配置文件，该文件用于指定许可证颁发机构的 URL。

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

- 在部署 ASAv 时，您可设置功能层和吞吐量级别。此时仅标准级别可用。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。

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

- 此外，在配置过程中，您还可以选择配置 HTTP 代理。

```
call-home
  http-proxy ip_address port port
```

Firepower 1000 和 2100

Firepower 1000 和 2100 默认配置包括名为“License”的 Smart Call Home 配置文件，该文件用于指定许可证颁发机构的 URL。

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

Firepower 4100/9300 机箱 上的 ASA

没有默认配置。您必须手动启用标准许可证层和其他可选许可证。

ASAv：配置智能软件许可

本节介绍如何为 ASAv 配置智能软件许可。选择以下方法之一：

过程

步骤 1 ASAv：配置常规智能软件许可，第 20 页。

步骤 2 ASAv：配置卫星智能软件许可，第 24 页。

步骤 3 ASAv：配置使用模式和 MSLA 智能软件许可，第 25 页

步骤 4 ASAv：配置永久许可证保留，第 28 页。

ASAv：配置常规智能软件许可

在部署 ASAv 时，您可以预配置设备并包含一个注册令牌，以便其向许可证颁发机构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 ASAv（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 ASAv 时预配置了 HTTP 代理服务器和许可证授权。您还可能在部署 ASAv 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

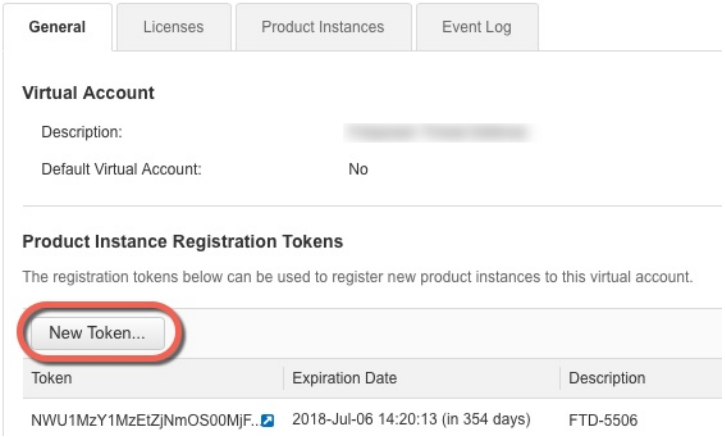
步骤 1 在智能软件管理器（思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

a) 点击**资产 (Inventory)**。

图 *2:* 资产

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

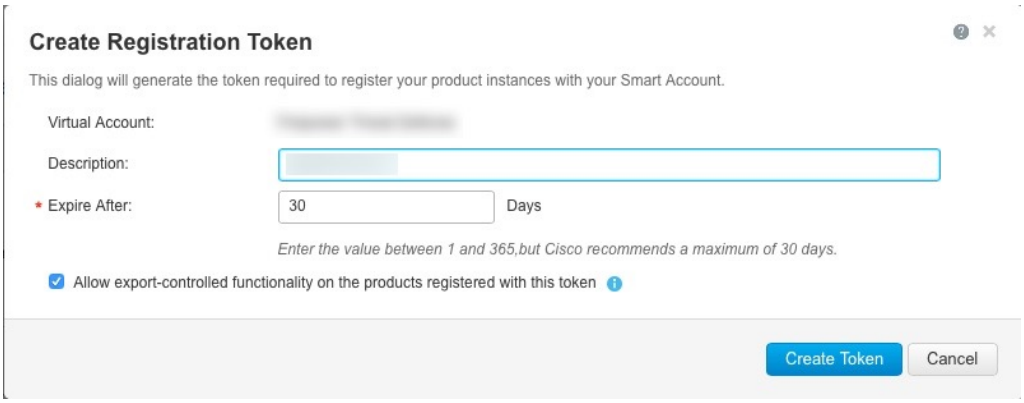
图 *3:* 新建令牌



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

- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

图 *4:* 创建注册令牌



系统将令牌添加到您的资产中。

d) 单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 *5:* 查看令牌

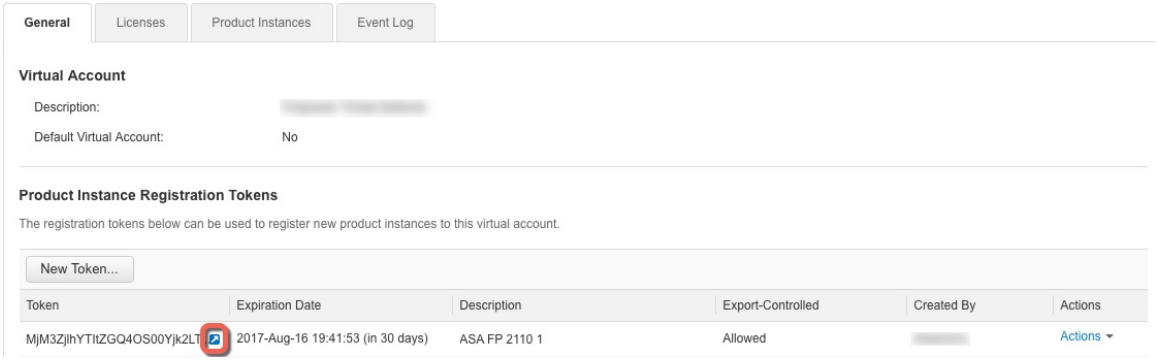
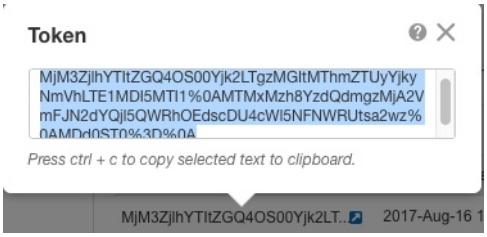


图 *6:* 复制令牌



步骤 2 （可选） 在 ASAv 上指定 HTTP 代理 URL：

call-home

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

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

示例：

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

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

仅标准层可用。

c) 设置吞吐量级别：

throughput level {**100M** | **1G** | **2G** | **10G** | **20G**}

示例：

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

a) 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 向许可证颁发机构注册 ASAv。

在注册 ASAv 时，许可证颁发机构会为 ASAv 与许可证颁发机构之间的通信颁发 ID 证书。它还会将 ASAv 分配到相应的虚拟帐户。通常，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 ASAv。

a) 在 ASAv 中输入注册令牌：

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

示例：

使用 **force** 关键字注册已注册但可能与许可证颁发机构不同步的 ASAv。例如，如果从智能软件管理器中意外删除了 ASAv，请使用 **force**。

ASAv 尝试向许可证颁发机构注册并请求对已配置的许可证授权进行授权。

示例：

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

ASAv：配置卫星智能软件许可

此程序适用于使用卫星智能软件许可服务器的 ASAv。

开始之前

从 Cisco.com 下载智能软件管理器卫星 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关详细信息，请参阅智能软件管理器卫星。

过程

步骤 1 请求卫星服务器上的注册令牌。

步骤 2 （可选） 在 ASA 上指定 HTTP 代理 URL：

call-home

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

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

示例：

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

步骤 3 更改许可证服务器 URL，以转至卫星服务器。

call-home

profile License

destination address http https://*satellite_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 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
```

ASA 将向卫星服务器注册并申请授权已配置的许可证授权。如果您的帐户允许，则卫星服务器还会应用强加密 (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... (FP2110-ASA-Std)                    1 AUTHORIZED
```

ASAv：配置使用模式和 MSLA 智能软件许可

此程序适用于在托管服务许可协议(MSLA)程序中注册的智能许可实用程序模式下的ASAv。在实用程序模式下，智能代理以时间单位跟踪许可授权的使用情况。智能代理每四小时向许可证卫星或服务器发送一次许可证使用报告。使用情况报告将转发到计费服务器，并向客户发送每月的许可证使用费账单。

开始之前

从Cisco.com下载智能软件管理器卫星OVA文件，并在VMware ESXi服务器上安装和配置此文件。有关详细信息，请参阅“智能软件管理器卫星”。

过程

步骤 1 请求卫星服务器上的注册令牌；请参阅 设备注册和令牌，第 59 页。

步骤 2 在 ASAv 上，为 MSLA 智能许可配置设备。

a) 指定要用于 MSLA 许可消息传送的智能传输 (HTTP)。

transport type *callhome smart*

示例：

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

重要事项 默认情况下，智能许可使用 Smart Call Home 基础设施与智能软件管理器通信。但是，Smart Call Home 不支持 MSLA。如果计划在 MSLA 标准实用程序模式下运行 ASAv，则必须配置智能传输。

b) 使用智能传输时，可以指定许可服务器或卫星的在URL，也可以选择使用默认 URL。或者，您可以为许可智能代理生成的许可证使用情况报告，指定第二个服务器/卫星目标。

transport url *transport-url* **default utility** *utility-url*

示例：

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

注释 如果未提供条目，则 **transport url** 设置默认为 *https://smartreceiver.cisco.com/licservice/license*。

c) （可选） 如果您的网络使用 HTTP 代理访问互联网，则必须为智能软件许可配置代理地址。

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

示例：

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

步骤 3 您可以选择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
```

步骤 4 配置实用程序许可信息，其中包括计费所需的客户信息。

a) 进入使用情况配置模式：

utility

示例：

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

b) 您可以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) 您可以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

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
```

步骤 5 （可选） 当 ASAv 需要在标准 MSLA 模式下运行时，请使用此命令。标准 MSLA 模式要求您将智能许可配置为使用智能传输。命令的否定版本会清除标准 MSLA 模式，并将 ASAv 置于默认实用程序模式，该模式可以使用 Smart Transport 或 Smart Call Home。

mode standard

示例：

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

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
```

使用 **show run license** 命令检查许可证状态和使用情况。

示例：

```
ciscoasa# show run license

license smart
 feature tier standard
 throughput level 2G
 transport type smart
 transport url http://10.196.155.133:80/Transportgateway/services/DeviceRequestHandler
 transport url utility http://10.196.155.133:80/Transportgateway/services/DeviceRequestHandler

 utility
 mode standard
 custom-id CUSTOM-ID-AUTOMATION1234
 customer-info id ID-AUTOMATION1234
 customer-info name NAME-AUTOMATION
 customer-info street KitCreekRoad
 customer-info city RTP
 customer-info state NC
 customer-info country USA
 customer-info postalcode 12345
```

ASAv：配置永久许可证保留

可以为 ASAv 分配永久许可证。本部分介绍在您停用 ASAv 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 ASAv 永久许可证，第 28 页

步骤 2 （可选）（可选）返还 ASAv 永久许可证，第 30 页

安装 ASAv 永久许可证

对于无法访问互联网的 ASAv，您可以向智能软件管理器请求永久许可证。

注释 对于永久许可证预留，您必须在停用 ASAv 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 ASAv。请参阅（可选）返还 ASAv 永久许可证，第 30 页。

注释 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，请确保已获得思科批准。
- 在 ASAv 启动之后，您必须请求永久许可证；您不能在 Day 0 配置期间安装永久许可证。

过程

步骤 1 在 ASAv CLI 中，启用永久许可证预留：

license smart reservation

示例：

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

删除了以下命令：

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

要使用常规智能许可，请使用此命令的 **no** 形式，然后重新输入上述命令。其他 Smart Call Home 配置保持不变，但未使用，因此您不需要重新输入这些命令。

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:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

您必须选择要在 ASAv 部署期间使用的型号级别 (ASAv5/ASAv10/ASAv30/ASAv50)。该型号级别会确定您请求的许可证。如果稍后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 ASAv 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 ASAv 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，则必须完成此程才能将该许可证应用于ASAv，然后，可以根据需要退回该许可证。请参阅（可选）返还 ASAv 永久许可证，第 30 页。

步骤 3 访问“Smart Software Manager Inventory”屏幕，点击 **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 **License Reservation**，并在框中键入 ASAv 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 ASAv 中输入授权码：

license smart reservation install *code*

示例：

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

ASAv 现在完全获得许可。

（可选）返还 ASAv 永久许可证

如果您不再需要永久许可证（例如，您要停用 ASAv 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 在 ASAv 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=
```

ASAv将立即变为未许可并进入Evaluation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**)，或更改 ASAv 型号级别（通过断开电源并更换 vCPU/RAM），则将无法重新显示此代码。确保捕获该代码以完成返还。

步骤 2 在智能软件管理器中查看 ASAv 通用设备标识符 (UDI)，这样可以找到此 ASAv 实例：

show license udi

示例：

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

步骤 3 访问智能软件管理器的 Inventory 屏幕，然后点击 **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 找到您想取消许可的 ASAv，依次选择 **Actions** > **Remove**，然后在方框中键入 ASAv 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 ASAv（常规和卫星）

取消注册 ASAv 会将 ASAv 从帐户中删除。ASAv 上的所有许可证授权和证书都将删除。您可能需要取消注册才能为新 ASAv 释放许可证。或者，可以将 ASAv 从智能软件管理器中删除。

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

过程

取消注册 ASAv：

license smart deregister

系统随即重新加载 ASAv。

（可选）续约 ASAv ID 证书或许可证授权（常规和卫星）

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

Firepower 1000、2100：配置智能软件许可

本节介绍如何为 Firepower 1000、 2100 配置智能软件许可。选择以下方法之一：

过程

步骤 1 Firepower 1000、2100：配置常规智能软件许可 ， 第 32 页。

您也可以（可选）取消注册 Firepower 1000、2100（常规和卫星） ， 第 43 页或（可选）续约 Firepower 1000、2100 ID 证书或许可证授权（常规和卫星） ， 第 43 页。

步骤 2 Firepower 1000、2100：配置卫星智能软件许可 ， 第 36 页。

您也可以（可选）取消注册 Firepower 1000、2100（常规和卫星） ， 第 43 页或（可选）续约 Firepower 1000、2100 ID 证书或许可证授权（常规和卫星） ， 第 43 页。

步骤 3 Firepower 1000、 2100：配置永久许可证保留 ， 第 39 页。

Firepower 1000、2100：配置常规智能软件许可

此程序适用于使用许可证颁发机构的 ASA。

过程

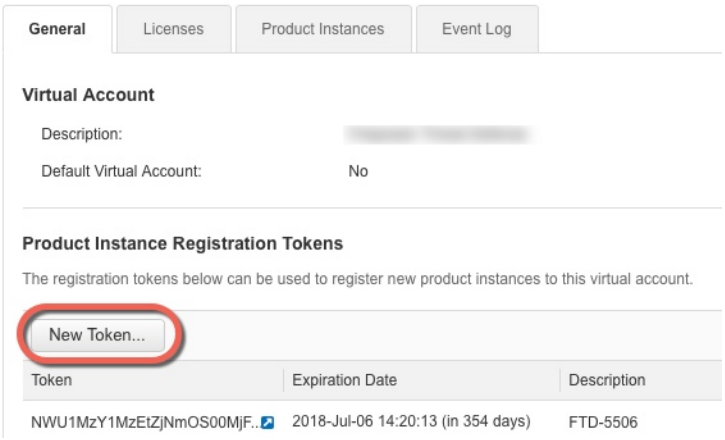
步骤 1 在智能软件管理器（思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

a) 点击**资产 (Inventory)**。

图 *7:* 资产

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

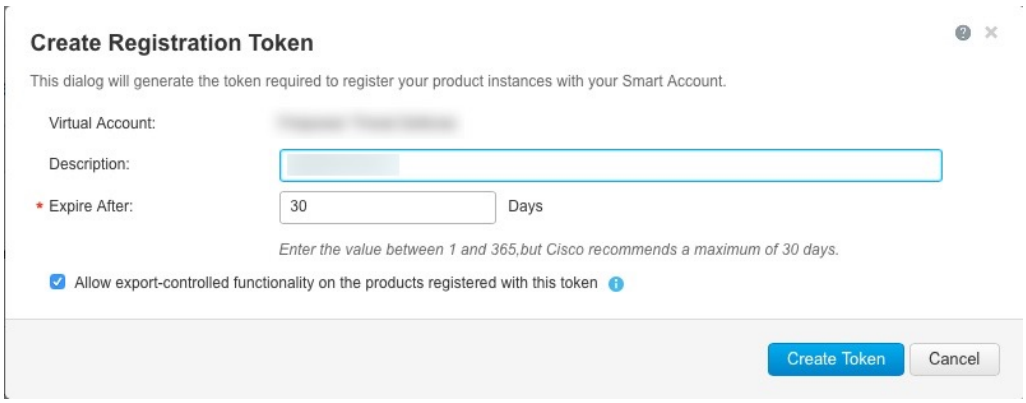
图 *8:* 新建令牌



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

- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

图 *9:* 创建注册令牌



系统将令牌添加到您的资产中。

d) 单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 *10:* 查看令牌

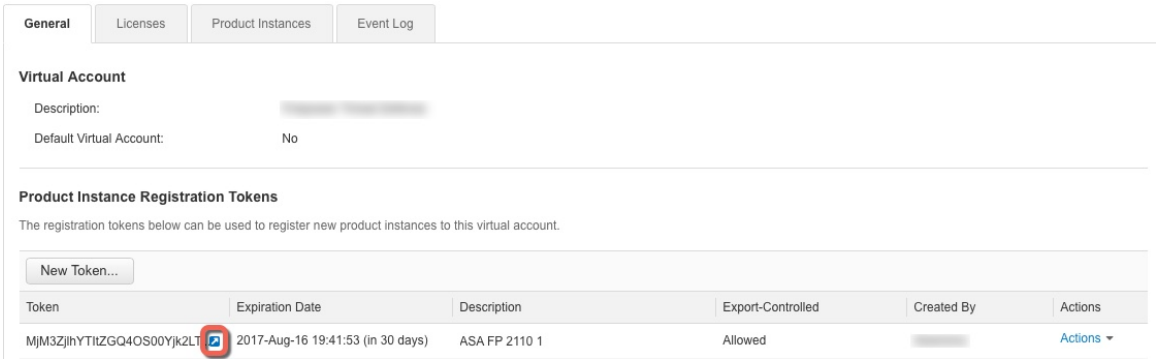
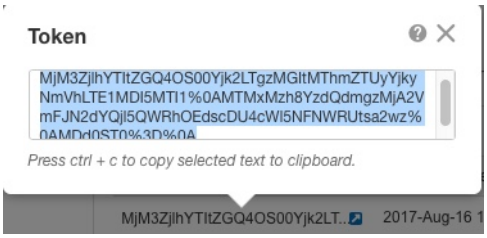


图 *11:* 复制令牌



步骤 2 （可选） 在 ASA 上指定 HTTP 代理 URL：

call-home

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

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

示例：

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

步骤 3 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) 设置功能层：

feature tier standard

仅标准许可证可用。层许可证是添加其他功能许可证的前提条件。

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 - 15 种情景
- Firepower 2110 - 25 种情景
- Firepower 2120 - 25 种情景
- Firepower 2130 - 30 种情景
- Firepower 2140 - 40 种情景

例如，如果 Firepower 2110 要使用最大值，即 25 种情景，请为情景数量输入 23；此值将与默认值 2 相加。

示例：

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

d) (Firepower 1010) 请求增强型安全许可证以启用主用/备用故障切换。

feature security-plus

示例：

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

e) （可选） 强加密协议通常不是必需的；例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证，但如果您知道自己需要，或者想要在帐户中跟踪此许可证的使用情况，可以启用此功能。

feature strong-encryption

示例：

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

步骤 4 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 将向注册机构注册并申请授权已配置的许可证授权。如果您的帐户允许，则许可证颁发机构还会应用强加密 (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... (FP2110-ASA-Std)                    1 AUTHORIZED
```

Firepower 1000、2100：配置卫星智能软件许可

此程序适用于使用卫星智能软件许可服务器的 ASA。

开始之前

从 Cisco.com 下载智能软件管理器卫星 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关详细信息，请参阅智能软件管理器卫星。

过程

步骤 1 请求卫星服务器上的注册令牌。

步骤 2 （可选） 在 ASA 上指定 HTTP 代理 URL：

call-home

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

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

示例：

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

步骤 3 更改许可证服务器 URL，以转至卫星服务器。

call-home

profile License

destination address http https://*satellite_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 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) 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。

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 - 15 种情景

- Firepower 2110 - 25 种情景
- Firepower 2120 - 25 种情景
- Firepower 2130 - 30 种情景
- Firepower 2140 - 40 种情景

例如，如果 Firepower 2110 要使用最大值，即 25 种情景，请为情景数量输入 23；此值将与默认值 2 相加。

示例：

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

d) (Firepower 1010) 请求增强型安全许可证以启用主用/备用故障切换。

feature security-plus

示例：

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

e) （可选） 强加密协议通常不是必需的；例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证，但如果您知道自己需要，或者想要在帐户中跟踪此许可证的使用情况，可以启用此功能。

feature strong-encryption

示例：

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

步骤 5 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 将向卫星服务器注册并申请授权已配置的许可证授权。如果您的帐户允许，则卫星服务器还会应用强加密 (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... (FP2110-ASA-Std)                     1 AUTHORIZED
```

Firepower 1000、 2100：配置永久许可证保留

您可以为 Firepower 1000、 2100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 Firepower 1000、2100 永久许可证， 第 39 页。

步骤 2 （可选） （可选）返还 Firepower 1000、2100 永久许可证， 第 42 页。

安装 Firepower 1000、2100 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标准许可证。

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 Firepower 1000、2100 永久许可证， 第 42 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 Firepower 1000、2100 永久许可证，第 42 页。

步骤 3 访问“Smart Software Manager Inventory”屏幕，点击 **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。

您需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

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) 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。

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 - 15 种情景
- Firepower 2110 - 25 种情景
- Firepower 2120 - 25 种情景
- Firepower 2130 - 30 种情景
- Firepower 2140 - 40 种情景

例如，如果 Firepower 2110 要使用最大值，即 25 种情景，请为情景数量输入 23；此值将与默认值 2 相加。

示例：

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

d) (Firepower 1010) 请求增强型安全许可证以启用主用/备用故障切换。

feature security-plus

示例：

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

e) （可选） 强加密协议通常不是必需的；例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证，但如果您知道自己需要，或者想要在帐户中跟踪此许可证的使用情况，可以启用此功能。

feature strong-encryption

示例：

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

（可选）返还 Firepower 1000、2100 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 60 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 Inventory 屏幕，然后点击 **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 Firepower 1000、2100（常规和卫星）

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Firepower1000、2100ID证书或许可证授权（常规和卫星）

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：的卫星智能软件许可

此程序适用于使用许可证颁发机构的机箱（卫星服务器用户），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。

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。

注释 对于 2.3.0 版以前的智能软件管理器卫星用户：强加密 (3DES/AES) 许可证默认未启用，因此在使用 ASA CLI 申请强加密许可证之前，您无法使用 ASDM 配置您的 ASA。在您执行此操作前，其他强加密功能也能使用，包括 VPN。

开始之前

对于 ASA 集群，您需要访问控制单元进行配置。查看 Firepower 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)。

- **仅对于 2.3.0 版以前的卫星服务器用户：**强加密 (3DES/AES)

feature strong-encryption

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。

ASAv

可在任何受支持的 ASAv vCPU/内存配置中使用任何 ASAv 许可证。这可让 ASAv 客户在各种各样的 VM 资源中运行。这还会增加受支持的 AWS 和 Azure 实例类型的数量。配置 ASAv VM 时，支持的 vCPU 最多为 8 个（如果是 VMware 和 KVM 上的 ASAv100，最多为 16 个）；支持的最大内存为 64GB。

重要事项 ASAv 的最低内存要求为 2GB。如果当前 ASAv 的内存少于 2GB，您将无法在不增加 ASAv VM 内存的情况下，从早期版本升级到 9.13(1) 或更高版本。您也可以使用最新版本重新部署新的 ASAv VM。

部署具有超过 1 个 vCPU 的 ASAv 时，ASAv 的最低内存要求是 4GB。

灵活的许可指导原则

- 许可功能和未许可平台功能的会话限制根据 VM 内存量设置。
- AnyConnect 和 TLS 代理的会话限制将由 ASAv 平台权限确定；会话限制不再与 ASAv 模型类型 (ASAv5/10/30/50/100) 关联。

  会话限制有最低内存要求；如果 VM 内存低于最低要求，会话限制将设置为内存量支持的最大数。
- 防火墙连接数、并行和 VLAN 是基于 ASAv 内存的平台限制。
- 没有授权限制；任何授权都可在任意组合的 vCPU（VMware 和 KVM 上最多为 8 或 16 个 ASAv100） 和内存（最多 64GB）上运行。
- 现有授权没有任何变化；授权 SKU 和显示名称将继续包括型号 (ASAv5/10/30/50/100)。
- 授权通过速度限制器设置最大吞吐量。

- 客户订购过程没有变化。

许可证	灵活的许可证
防火墙许可证	
僵尸网络流量过滤器	启用
运营商	启用
Total TLS Proxy Sessions	100 Mbps 授权：500 1 Gbps 授权：500 2 Gbps 授权：1000 10 Gbps 授权：10,000 20 Gbps 授权：20,000
VPN 许可证	
AnyConnect 对等体	100 Mbps 授权：50 1 Gbps 授权：250 2 Gbps 授权：750 10 Gbps 授权：10,000 20 Gbps 授权：20,000
其他 VPN 对等体	100 Mbps 授权：50 1 Gbps 授权：250 2 Gbps 授权：1000 10 Gbps 授权：10,000 20 Gbps 授权：20,000
VPN 对等体总数（包括所有类型）	100 Mbps 授权：50 1 Gbps 授权：250 2 Gbps 授权：1000 10 Gbps 授权：10,000 20 Gbps 授权：20,000
通用许可证	

许可证	灵活的许可证
吞吐量级别	ASAv STD 100M-100 Mbps ASAv STD 1G-1 Gbps ASAv STD 2G-2 Gbps ASAv STD 10G-10 Gbps ASAv STD 20G-20 Gbps
加密	基本 (DES) 或强 (3DES/AES)，具体取决于帐户的导出合规性设置
故障切换	主用/备用
安全情景	不支持
集群	不支持

vCPU、RAM	支持的 vCPU 最多为 8 个（如果是 VMware 和 KVM 上的 ASAv100，最多为 16 个）；支持的最大内存为 64GB。您可以使用 vCPU 和内存的任意组合部署任何 ASAv 授权级别。
	• ASAv 的最低内存要求为 2GB。
	• 部署具有超过 1 个 vCPU 的 ASAv 时，ASAv 的最低内存要求是 4GB。
	• 平台限制由所需的内存量实施。
	• 会话限制取决于部署的授权类型，并由最低内存要求实施。
	  • 100 Mbps 授权：2GB 至 7.9GB
	  • 1 Gbps 授权：2GB 至 7.9GB
	  • 2 Gbps 授权：8GB 至 15.9GB
	  • 10 Gbps 授权：16GB 至 31.9GB
	  • 20 Gbps 授权：32GB 至 64GB

平台限制

并行防火墙连接数和 VLAN 是基于 ASAv 内存的平台限制。

注释 当 ASAv 处于“未获得许可”状态时，防火墙连接数上限为 100。获得任何授权的许可后，连接数将遵循平台限制。ASAv 的最低内存要求为 2GB。

表 *1:* 平台限制

ASAv 内存	并发防火墙连接数	**VLAN**
2 GB 至 7.9 GB	100,000	50
8 GB 至 15.9 GB	500,000	200
16 GB 至 31.9 GB	2,000,000	1024
32 GB 至 64 GB	4,000,000	1024

Firepower 1010

下表显示 Firepower 1010 已获许可的功能。

许可证	标准许可证	
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		
AnyConnect 对等体	未获得许可	可选的 *AnyConnect Plus* 或 *Apex* 许可证，最大数量：*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	基本 (DES) 或强 (3DES/AES)，具体取决于帐户的导出合规性设置	
增强型安全（故障切换）	已禁用	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	标准许可证	
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 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		
AnyConnect 对等体	未获得许可	可选的 *AnyConnect Plus* 或 *Apex* 许可证，最大数量： *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	

许可证	标准许可证	
安全情景	2	可选许可证，最多： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*
集群	不支持。	
最大 VLAN 数量	1024	

Firepower 2100 系列

下表显示 Firepower 2100 系列已获许可的功能。

许可证	标准许可证	
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 2110：1,000,000 Firepower 2120：1,500,000 Firepower 2130：2,000,000 Firepower 2140：3,000,000	
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 2110：4,000 Firepower 2120：8,000 Firepower 2130：8,000 Firepower 2140：10,000	
VPN 许可证		
AnyConnect 对等体	未获得许可	可选的 *AnyConnect Plus* 或 *Apex* 许可证，最大数量： *Firepower 2110：1,500* *Firepower 2120：3,500* *Firepower 2130：7,500* *Firepower 2140：10,000*

许可证	标准许可证	
其他 VPN 对等体数	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
VPN 对等体总数（包括所有类型）	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
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，最大数量（以 *5* 或 *10* 个为增量）： *Firepower 2110：25* *Firepower 2120：25* *Firepower 2130：30* *Firepower 2140：40*
集群	不支持。	
最大 VLAN 数量	1024	

Firepower 4100 系列 ASA 应用程序

下表显示 Firepower 4100 系列 ASA 应用程序的许可功能。

许可证	标准许可证
防火墙许可证	
僵尸网络流量过滤器	不支持。

许可证	标准许可证	
并发防火墙连接数	Firepower 4110：10,000,000 Firepower 4112：10,000,000 Firepower 4115：15,000,000 Firepower 4120：15,000,000 Firepower 4125：25,000,000 Firepower 4140：25,000,000 Firepower 4145：40,000,000 Firepower 4150：35,000,000	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	Firepower 4110：10,000 所有其他：15,000	
VPN 许可证		
AnyConnect 对等体	未获得许可	可选的 *AnyConnect Plus* 或 *Apex* 许可证： *Firepower 4110：10,000* 所有其他：*20,000*
其他 VPN 对等体	Firepower 4110：10,000 所有其他：20,000	
VPN 对等体总数（包括所有类型）	Firepower 4110：10,000 所有其他：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* 个，以 *10* 为单位递增
集群	启用	
最大 VLAN 数量	1024	

Firepower 9300 ASA 应用

下表显示 Firepower 9300 ASA 应用的许可功能。

许可证	标准许可证	
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，对于包含3个模块的机箱，最高可达70,000,000 Firepower 9300 SM-48：60,000,000，对于包含3个模块的机箱，最高为70,000,000 Firepower 9300 SM-44：60,000,000，对于具有3个模块的机箱，最高可达70,000,000 Firepower 9300 SM-40：60,000,000，对于具有3个模块的机箱，最高为70,000,000 Firepower 9300 SM-36：60,000,000，对于包含3个模块的机箱，最高为70,000,000 Firepower 9300 SM-24：55,000,000，对于包含 3 个模块的机箱，最高为 70,000,000	
Carrier	已禁用	可选许可证：运营商
TLS 代理会话总数	15,000	
VPN 许可证		
AnyConnect 对等体	未获得许可	可选的 *AnyConnect Plus* 或 *Apex* 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* 个，以 *10* 为单位递增
集群	启用	
最大 VLAN 数量	1024	

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。

查看当前许可证

如需查看许可证，请参阅以下命令：

- **show license features**

  以下示例显示的是只有一个基础许可证的 ASAv（无当前许可证授权）：

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

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 ASAv 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 ASAv 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 ASAv 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 ASAv 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 ASAv 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 ASAv 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，设备会向思科许可证颁发机构进行注册。当设备向令牌注册时，许可证颁发机构会颁发ID证书，用于在设备与许可证颁发机构之间进行通信。此证书有效期为 1 年，但需要每 6 个月续签一次。

与许可证颁发机构的定期通信

设备每30天与许可证颁发机构进行通信。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。

ASAv

ASAv 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，您应该联系许可颁发机构，否则您的 ASAv 将不合规。

Firepower 1000

Firepower 1000 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，您必须联系许可证颁发机构，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。

Firepower 2100

Firepower 2100 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，您必须联系许可证颁发机构，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。

Firepower 4100/9300

Firepower 4100/9300 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，您必须联系许可证颁发机构，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：

- ASAv - ASAv 不受影响。
- Firepower 1000 - 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，基于标准许可证限制的现有情景可以继续运行，您可以修改它们的配置，但无法添加新情景。如果首次注册时没有足够的标准许可证，则无法配置任何许可功能，包括强加密功能。
- Firepower 2100 - 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，基于标准许可证限制的现有情景可以继续运行，您可以修改它们的配置，但无法添加新情景。如果首次注册时没有足够的标准许可证，则无法配置任何许可功能，包括强加密功能。
- Firepower 4100/9300 - 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，基于标准许可证限制的现有情景可以继续运行，您可以修改它们的配置，但无法添加新情景。如果首次注册时没有足够的标准许可证，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许可颁发机构的 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许可证颁发机构的目的地址 URL。除非获得 Cisco TAC 的指示，否则不应更改许可证颁发机构 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 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。

智能软件许可历史记录

功能名称	平台版本	说明
ASAv100 永久许可证保留	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。
ASAv MSLA 支持	9.13(1)	ASAv 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**
ASAv 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 ASAv vCPU/内存配置中使用任何 ASAv 许可证。AnyConnect 和 TLS 代理的会话限制将由安装的 ASAv 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 上故障切换对的许可	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 ASAv 短字符串增强的永久许可证保留	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。
卫星服务器对 ASAv 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。

功能名称	平台版本	说明
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。
ASAv 永久许可证保留	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 ASAv 永久许可证。 在 9.6(2) 中，我们还为 Amazon Web 服务上的 ASAv 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保留，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，ASAv 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**
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**

功能名称	平台版本	说明
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**
适用于 ASAv 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，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。 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**