许可证：用于 ISA 3000 的产品授权密钥许可

许可证指定在给定 ASA 上启用的选项。本文档介绍所有物理 ISA 3000 的产品授权密钥 (PAK) 许可证。有关其他型号，请参阅 许可证：智能软件许可。

关于 PAK 许可证

许可证指定在给定 ASA 上启用的选项。它由一个表示 160 位（5 个 32 位字或 20 个字节）值的激活密钥表示。该值对序列号（11 个字符的字符串）和已启用的功能进行编码。

预安装的许可证

默认情况下，ASA 已预安装了一个许可证。此许可证可能是基础许可证，您要向其添加更多许可证，或者其可能已经安装所有许可证，具体取决于您的订购以及供应商为您安装的内容。

相关主题

监控 PAK 许可证， 第 23 页

永久许可证

您可以安装一个永久激活密钥。永久激活密钥在单个密钥中包含所有许可功能。如果您还安装了基于时间的许可证，则 ASA 会将永久许可证和基于时间的许可证合并为运行许可证。

相关主题

永久许可证与基于时间的许可证的合并方式， 第 2 页

基于时间的许可证

除永久许可证以外，您还可以购买基于时间的许可证，或者接收具有时间限制的评估许可证。例如，您可能会购买基于时间的 Secure Client 高级版许可证，以处理并发 SSL VPN 用户数的短期激增。

基于时间的许可证激活准则

- 您可以安装多个基于时间的许可证，包括同一功能的多个许可证。但是，每个功能一次只能有一个基于时间的许可证处于活动状态。非活动许可证保持已安装状态，并可随时使用。例如，如果安装一个 1000 会话的 Secure Client 高级版许可证和一个 2500 会话的 Secure Client 高级版许可证，则其中仅有一个许可证可处于活动状态。
- 如果激活在密钥中具有多个功能的评估许可证，则无法为所包含的其中一个功能也同时激活另一基于时间的许可证。

基于时间的许可证计时器工作方式

- 当在 ASA 上激活基于时间的许可证时，其计时器便开始倒计时。
- 如果在基于时间的许可证超时之前停止对其进行使用，则计时器会停止。仅当重新激活基于时间的许可证时，计时器才会再次启动。
- 如果基于时间的许可证处于活动状态，并且您关闭 ASA，则计时器会停止倒计时。仅当 ASA 正在运行时，基于时间的许可证才会倒计时。系统时钟设置不影响许可证；只有 ASA 正常运行时间会计入许可证持续时间。

永久许可证与基于时间的许可证的合并方式

激活基于时间的许可证时，通过永久许可证与基于时间的许可证获得的功能将合并以形成正在运行的许可证。永久许可证与基于时间的许可证的合并方式取决于许可证的类型。下表列出了每个功能许可证的合并规则。

注释 即使使用了永久许可证，如果基于时间的许可证处于活动状态，也会继续倒计时。

表 *1:* 基于时间的许可证合并规则

基于时间的功能	合并许可证规则
Secure Client 高级会话	使用基于时间的许可证或永久许可证两者中的较高值。例如，如果永久许可证是 1000 个会话，基于时间的许可证是 2500 个会话，则会启用 2500 个会话。通常，不会安装功能弱于永久许可证的基于时间的许可证，但是，如果您这么做，则会使用永久许可证。

基于时间的功能	合并许可证规则
统一通信代理会话	基于时间的许可证会话会添加到永久会话中，最高值为平台限制。例如，如果永久许可证为 2500 个会话，基于时间的许可证为 1000 个会话，则只要基于时间的许可证处于活动状态，就会启用 3500 个会话。
其他所有	使用基于时间的许可证或永久许可证两者中的较高值。对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。对于具有数字层的许可证，将使用较高的值。通常，不会安装功能弱于永久许可证的基于时间的许可证，但是，如果您这么做，则会使用永久许可证。

相关主题

监控 PAK 许可证，第 23 页

堆叠基于时间的许可证

在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，许可证没有到期尤为重要。ASA 允许堆叠基于时间的许可证，从而让您不必担忧许可证到期或由于提前安装了新许可证而损害许可证上的时间。

当安装与已安装的许可证相同的基于时间的许可证时，许可证会进行合并，并且持续时间等于合并后的持续时间。

例如：

1. 您安装有一个 8 周的 1000 会话 Secure Client 高级版许可证，并且该许可证已使用 2 周（剩余 6 周）。
2. 然后，您又安装了另一个 8 周 1000 个会话许可证，许可证合并具有 14 周 1000 个会话（8 周加上 6 周）。

如果许可证不同（例如，1000 会话 Secure Client 高级版许可证和 2500 会话许可证），则许可证 不会 合并。由于每个功能仅能有一个基于时间的许可证处于活动状态，这些许可证中仅有一个许可证可以处于活动状态。

虽然不能合并不相同的许可证，但在当前许可证到期时，ASA 会自动激活已安装的功能相同的许可证（如果可用）。

相关主题

激活或停用密钥，第 14 页
基于时间的许可证到期，第 3 页

基于时间的许可证到期

当某个功能的当前许可证到期时，ASA 会自动激活同一功能的已安装许可证（如果适用）。如果没有其他适用于此功能的基于时间的许可证，则会使用永久许可证。

如果为某个功能安装了多个额外的基于时间的许可证，则ASA会使用其找到的第一个许可证；将会使用哪个许可证不是用户可配置的，而是取决于内部操作。如果您希望使用的许可证不是ASA激活的基于时间的许可证，则必须手动激活您希望使用的许可证。

例如，您有一个基于时间的 2500 个会话 Secure Client 高级许可证（活动）、一个基于时间的 1000 个会话 Secure Client 高级许可证（非活动），以及一个永久的 500 个会话的 Secure Client 高级许可证。当 2500 个会话许可证到期时，ASA 会激活 1000 个会话许可证。在 1000 个会话许可证到期后，ASA 会使用 500 个会话永久许可证。

相关主题

激活或停用密钥，第 14 页

许可证说明

以下部分包括有关许可证的其他信息。

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

Secure Client Advantage或 Premier 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。仅 仅限 Secure Client VPN 许可证适用于特定的 ASA。请参阅 https://www.cisco.com/go/license，并单独为每个 ASA 分配 PAK。将生成的激活密钥应用于 ASA 时，会将 VPN 功能切换到允许的最大值，但共享该许可证的所有 ASA 中唯一用户的实际数量不应超出此许可证限制。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)

注释 Secure Client Premier 许可证是唯一支持多语境模式的 Secure Client Premier 许可证。此外，在多情景模式下，此许可证必须应用于故障转移对中的每台设备；该许可证不进行聚合。

其他 VPN 许可证

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。

合并后的各个类型的 VPN 会话总数

- 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。

VPN 负载均衡

VPN 负载均衡需要强加密 (3DES/AES) 许可证。

传统 VPN 许可证

有关许可的所有相关信息，请参阅 Secure Client补充最终用户许可协议 。

注释 Secure Client Premier 许可证时多情景模式下支持的唯一 Secure Client 许可证；您无法使用默认或传统许可证。

加密许可证

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。

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
```

共享 Secure Client 高级版许可证（AnyConnect 3 及更早版本）

注释 AnyConnect 4 及更高版本的许可不支持 ASA 上的共享许可证功能。 Secure Client 许可证是共享的，不再需要共享服务器或参与者许可证。

通过共享许可证，您可以购买大量的 Secure Client 高级会话，并且通过将一组 ASA 中的一个 ASA 配置为共享许可服务器，将剩余 ASA 配置为共享许可参与者，来根据需要在这组 ASA 之间共享会话。

故障转移

除一些例外情况之外，故障转移设备不要求每台设备上具有相同的许可证。对于早期版本，请参阅您的版本的许可文档。

故障转移许可证要求和例外

对于绝大多数型号，故障转移设备不要求每个设备上具有同一许可证。如果您在两台设备上都有许可证，则这两个许可证会合并为一个运行故障转移集群许可证。此规则存在一些例外情况。有关故障转移的具体许可要求，请参阅下表。

型号	许可证要求
ASA 虚拟	请参阅 ASAv 的故障转移许可证。
Firepower 1010	两个设备上都有增强型安全许可证。请参阅Firepower 1010 的故障转移许可证。
Firepower 1100	请参阅Firepower 1100 的故障转移许可证。

型号	许可证要求
Firepower 2100	请参阅Firepower 2100 的故障转移许可证。
Cisco Secure Firewall 3100	请参阅Cisco Secure Firewall 3100 的故障转移许可证。
Firepower 4100/9300	请参阅适用于 Firepower 4100/9300 的故障转移许可证。
ISA 3000	两个设备上都有增强型安全许可证。 **注释** 每台设备必须拥有相同的加密许可证。

注释 需要有效的永久密钥；在极少数情况下，在 ISA 3000 可以删除您的 PAK 身份验证密钥。如果密钥全部由 0 组成，则需要重新安装有效的身份验证密钥，然后才能启用故障转移。

如何合并故障转移或许可证

对于故障转移对，每台设备上的许可证会合并为单个运行集群许可证。如果您为每台设备购买单独的许可证，则合并的许可证使用以下规则：

- 对于具有数字层（例如，会话数）的许可证，每台设备的许可证的值会合并，最高值为平台限制。如果正在使用的所有许可证都基于时间，则许可证将同时倒计时。

  例如，对于故障转移：

  - 您有两台 ASA，每台安装了 10 个 TLS 代理会话；许可证将进行合并以获得总共 20 个 TLS 代理会话。
  - 您有一台具有 1000 个 TLS 代理会话的 ASA，以及另一台具有 2000 个会话的 ASA 5545-X；由于平台限制为 2000 个，因此合并的许可证可允许 2000 个 TLS 代理会话。

- 对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。
- 对于启用或禁用的基于时间的许可证（并且没有数字层），持续时间是所有许可证的合并后的持续时间。主/控制单位首先对其许可证进行倒计时，当其许可证到期时，辅助/数据单位开始对其许可证进行倒计时，依此类推。

相关主题

监控 PAK 许可证，第 23 页

故障转移或设备之间的通信丢失

如果设备丢失通信超过 30 天，则每台设备将还原到本地安装的许可证。在 30 天宽限期内，所有设备将继续使用合并的运行许可证。

如果在 30 天的宽限期内恢复通信，则对于基于时间的许可证，将从主/主许可证中减去耗用时间；如果主/主许可证已到期，则仅在此时辅助/从属许可证才会开始倒计时。

如果在30天内没有恢复通信，则对于基于时间的许可证，将从所有设备许可证（如果已安装）中减去耗用时间。它们会被视为独立许可证，不会受益于合并后的许可证。耗用时间包括 30 天的宽限期。

升级故障转移对

由于故障转移对不要求在两台设备上具有同一许可证，因此可以将新许可证应用于每台设备而不会产生任何停机时间。如果应用要求重新加载的永久许可证，则可以在重新加载时故障转移到另一台设备。如果两台设备都需要重新加载，则可以将其分开重新加载，以便不会产生停机时间。

相关主题

激活或停用密钥，第 14 页

无负载加密型号

您可以购买一些具有无负载加密功能的型号。如要出口至某些国家/地区，则在 ASA 系列上不能启用负载加密。ASA 软件可感知无负载加密型号，并会禁用以下功能：

- 统一通信
- VPN

您仍然可以安装强加密 (3DES/AES) 许可证，以便用于管理连接。例如，可以使用 ASDM HTTPS/SSL、SSHv2、Telnet 和 SNMPv3。

当您查看许可证时，将不会列出 VPN 许可证和统一通信许可证。

相关主题

监控 PAK 许可证，第 23 页

许可证 FAQ

我是否可以激活多个基于时间的许可证？

是。对于每个功能，您可以一次使用一个基于时间的许可证。

我是否可以“堆叠”基于时间的许可证，以便在时间限制解除时，将自动使用下一个许可证？

是。对于相同的许可证，当安装多个基于时间的许可证时，时间限制会合并。对于不相同的许可证（例如一个 1000 会话 Secure Client 高级版许可证和一个 2500 会话许可证），ASA 将自动激活它所发现的适用于此功能的基于下次的许可证。

我是否可以在使基于时间的许可证保持活动的同时，安装新的永久许可证？

是。激活永久许可证不会影响基于时间的许可证。

对于故障转移，我是否可以将共享许可服务器用作主设备，并将共享许可备用服务器用作辅助设备？

否。辅助设备具有与主设备相同的运行许可证；对于共享许可服务器，它们需要服务器许可证。备用服务器需要参与者许可证。备用服务器可以处于由两台备用服务器组成的一个单独故障转移对中。

我是否需要为故障转移对中的辅助设备购买相同的许可证？

否。从版本 8.3(1) 开始，不必在两台设备上拥有匹配的许可证。通常，您仅为主设备购买许可证；辅助设备在变为主用状态时会继承主许可证。对于您在辅助设备上也有独立许可证的情况（例如，如果您为版本 8.3 之前的软件购买了匹配的许可证），这些许可证会合并为运行故障转移集群许可证，其数量最高值为型号限制。

除共享型 AnyConnect 高级版许可证之外，我是否可以使用基于时间的或永久的 Secure Client 高级版许可证？

是。仅在本地安装的许可证（基于时间的许可证或永久许可证）中的会话用尽后，才会使用共享许可证。

注释 在共享许可服务器上，不使用永久 Secure Client 高级版许可证；但您可以与共享许可服务器许可证同时使用基于时间的许可证。在这种情况下，基于时间的许可证会话仅适用于本地 Secure Client 高级版会话；不能将其添加到共享许可池供参与者使用。

PAK 许可证准则

情景模式准则

在多情景模式下，请在系统执行空间中应用激活密钥。

故障转移准则

请参阅故障转移，第 6 页。

型号准则

- 仅在 ASA 虚拟 上支持智能许可。
- 在 ASA 虚拟、ASA 5506-X、ASA 5508-X 和 ASA 5516-X 上不支持共享许可。
- ASA 5506-X 和 ASA 5506W-X 不支持基于时间的许可证。

升级和降级准则

如果从任何之前版本升级到最新版本，则您的激活密钥保持兼容。但如果要维护降级功能，则可能会遇到问题：

- 降级到版本 8.1 或更早版本 - 在升级后，如果激活在版本 *8.2* 之前引入的其他功能许可证，则执行降级后激活密钥会继续与早期版本兼容。但是，如果激活在版本 *8.2* 或更高版本中引入的功能许可证，则激活密钥不会向后兼容。如果您有不兼容的许可证密钥，请参阅以下准则：
  - 如果以前输入了早期版本的激活密钥，则 ASA 会使用该密钥（没有您在版本 8.2 或更高版本中激活的任何新许可证）。
  - 如果您有新系统且没有早期的激活密钥，则需要请求与早期版本兼容的新激活密钥。
- 降级到版本 8.2 或更早版本 - 版本 8.3 中引入了更稳健的基于时间的密钥用法以及故障转移许可证变更：
  - 如果您有多个基于时间的激活密钥处于活动状态，则在降级后，只有最新激活的基于时间的密钥可以处于活动状态。所有其他密钥都会变为非活动状态。如果最后的基于时间的许可证是用于版本 8.3 中引入的功能，则该许可证即使无法在早期版本中使用，也仍会保持活动状态。重新输入永久密钥或有效的基于时间的密钥。
  - 如果在故障转移对上有不匹配的许可证，则降级将禁用故障转移。即使密钥匹配，所使用的许可证也将不再是合并许可证。
  - 如果您安装有一个基于时间的许可证，但是它用于版本 8.3 中引入的功能，则在降级之后，该基于时间的许可证保持活动状态。您需要重新输入永久密钥，以禁用该基于时间的许可证。

其他准则

- 激活密钥不会存储在配置文件中；它会以隐藏文件的形式存储在闪存中。
- 激活密钥会绑定到设备的序列号。功能许可证无法在设备之间转移（除非发生硬件故障）。如果您由于硬件故障而必须更换设备，并且思科 TAC 涵盖该设备，请联系思科许可团队，以便将您的现有许可证转移至新的序列号。思科许可团队将要求您提供产品许可密钥参考编号和现有序列号。
- 用于许可的序列号显示在 **show version** 输出中。此序列号与印制在硬件外部的机箱序列号不同。机箱序列号用于技术支持，但不用于许可。
- 一旦购买，您将无法退还许可证来获取退款或已升级的许可证。
- 在单个设备上，无法将用于同一功能的两个单独许可证合并；例如，如果您购买了一个 25 个会话 SSL VPN 许可证，此后又购买了 50 个会话许可证，则无法使用 75 个会话；您可以使用最多 50 个会话。（您能以升级价格购买更大的许可证，例如从 25 个到 75 个会话；应将这种升级与将两个单独许可证合并区分开来）。
- 虽然您可以激活所有许可证类型，但有些功能互不兼容。对于 AnyConnect 高级版许可证，此许可证与以下许可证不兼容：AnyConnect 高级版许可证、共享型 AnyConnect 高级版许可证以及高级终端评估许可证。默认情况下，如果安装了 AnyConnect 高级版许可证（如果其适用于您的型号），则会使用该许可证，而不是上述许可证。您可以依次使用 **webvpn** 和 **no anyconnect-essentials** 命令，在配置中禁用 AnyConnect 基础版许可证，以恢复使用其他许可证。

配置 PAK 许可证

本节介绍如何获取激活密钥以及如何将其激活。您也可以停用密钥。

订购许可证 PAK 并获取激活密钥

要在 ASA 上安装许可证，您需要生产授权密钥，您可以向 Cisco.com 注册该密钥以获取激活密钥。然后，可以在 ASA 上输入激活密钥。每个功能许可证都需要一个单独的生产授权密钥。PAK 合并在一起可为您提供一个激活密钥。您可能已随设备的包装箱收到所有的许可证 PAK。ASA 预安装了基础许可证和增强型安全许可证，以及强加密 (3DES/AES) 许可证（如果您有资格使用该许可证）。如果需要手动请求强机密许可证（免费），请访问 http://www.cisco.com/go/license。

开始之前

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

如果您还没有帐户，请设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

过程

步骤 1 要购买额外许可证，请参阅 http://www.cisco.com/go/ccw。请参阅以下 Secure Client 订购指南和常见问题解答：

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

订购许可证后，您会收到一封包含产品授权密钥 (PAK) 的邮件。对于 Secure Client 许可证，您将收到多用途 PAK，该 PAK 可应用于多个使用相同用户会话池的 ASA。有时，PAK 邮件可能需要几天才能收到。

步骤 2 通过输入以下命令获取 ASA 的序列号。

show version | grep Serial

许可使用的序列号与硬件铭牌上标示的机箱序列号不同。机箱序列号用于获取技术支持，而非获取许可。

步骤 3 要获取激活密钥，请转至以下许可网站：

http://www.cisco.com/go/license

步骤 4 系统提示时，输入以下信息：

- 产品授权密钥（如果您有多个密钥，请先输入其中一个密钥。您必须单独输入每个密钥。）
- ASA 的序列号

- 您的邮件地址

系统会自动生成激活密钥，并将其发送到您提供的邮件地址。此密钥包含迄今为止已注册的永久许可证的所有功能。对于基于时间的许可证，每个许可证具有单独的激活密钥。

步骤 5 如果您有其他产品授权密钥，请针对每个产品授权密钥重复此过程。输入所有产品授权密钥后，所提供的最终激活密钥会包含已注册的所有永久功能。

步骤 6 根据激活或停用密钥，第 14 页安装激活密钥。

获取强加密许可证

要使用 ASDM（和许多其他功能），您需要安装强加密 (3DES/AES) 许可证。如果 ASA 未预装强加密许可证，您可以免费申请一个。您必须符合所在国家/地区的强加密许可证条件。

过程

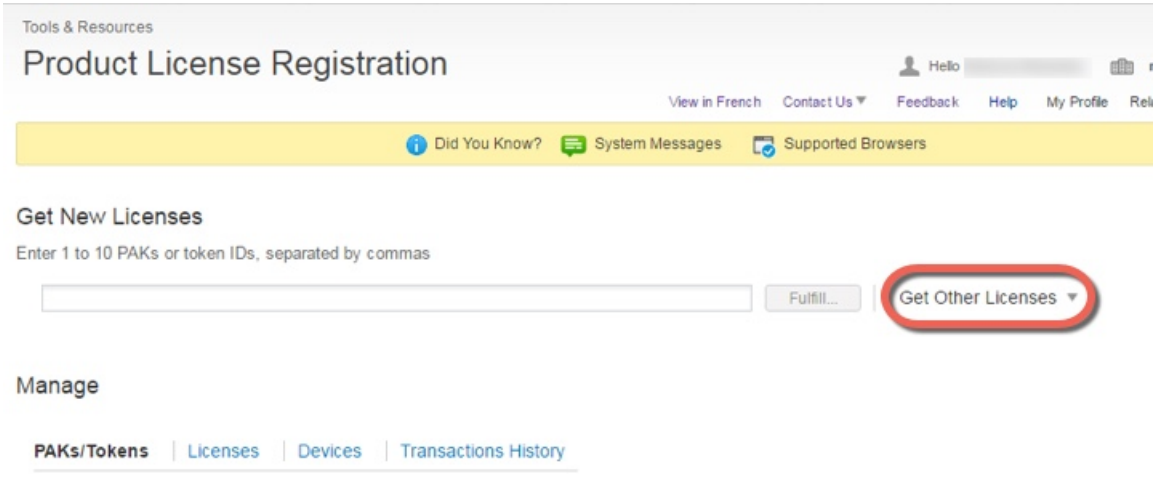
步骤 1 通过输入以下命令获取 ASA 的序列号：

show version | grep Serial

此序列号与印制在硬件外部的机箱序列号不同。机箱序列号用于技术支持，但不用于许可。

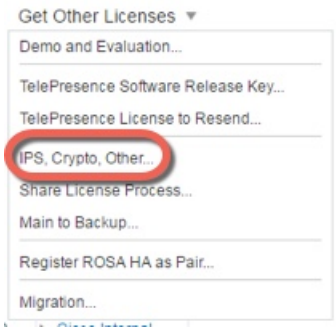
步骤 2 访问 https://www.cisco.com/go/license，然后点击**获取其他许可证**。

图 *1:* 获取其他许可证 *(Get Other Licenses)*



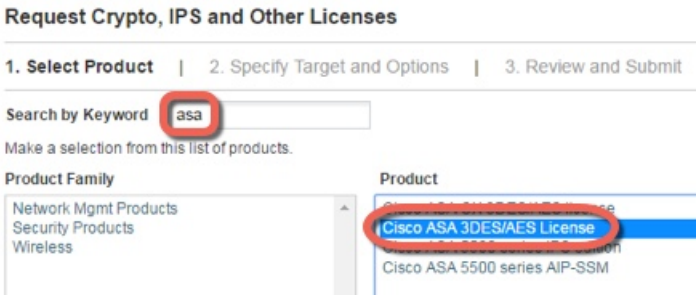
步骤 3 选择 **IPS, Crypto, Other**。

图 *2: IPS*、加密、其他 *(IPS, Crypto, Other)*



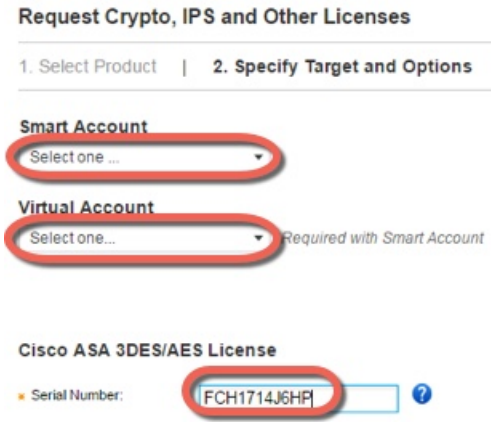
步骤 4 在 **Search by Keyword** 字段中，输入 **asa**，并选择 **Cisco ASA 3DES/AES License**。

图 *3:* 思科 ***ASA 3DES/AES*** 许可证 *(Cisco ASA 3DES/AES License)*



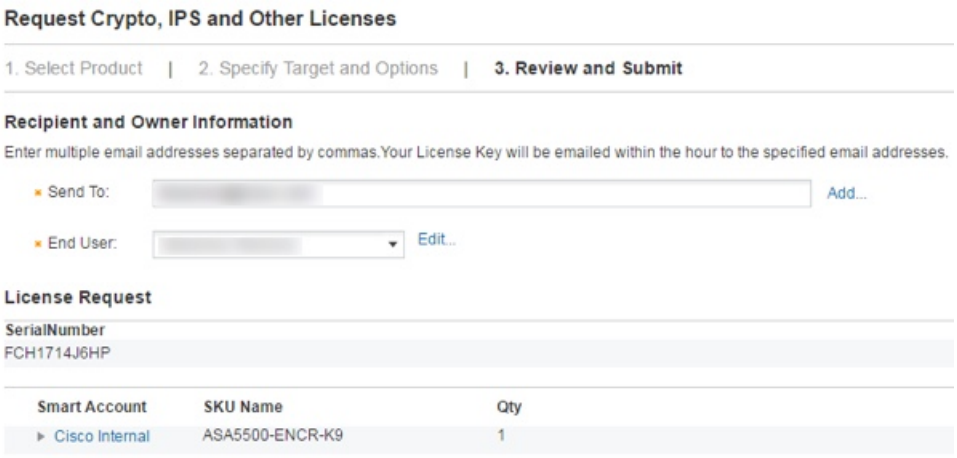
步骤 5 选择您的**智能帐户 (Smart Account)**、**虚拟帐户 (Virtual Account)**，输入 ASA 序列号 **(Serial Number)**，然后点击**下一步 (Next)**。

图 *4:* 智能帐户 *(Smart Account)*、虚拟帐户 *(Virtual Account)* 和序列号 *(Serial Number)*



步骤 6 系统将自动填充您的 Send To 邮箱地址和 End User 名称；必要时输入其他邮箱地址。选中**我同意 (I Agree)** 复选框，然后点击**提交 (Submit)**。

图 *5:* 提交



步骤 7 之后，您将会收到一封包含激活密钥的邮件，但您也可以立即从**管理 (Manage)** > **许可证 (Licenses)** 区域下载该密钥。

步骤 8 根据激活或停用密钥，第 14 页应用激活密钥。

激活或停用密钥

本节介绍如何输入新的激活密钥，以及如何激活和停用基于时间的密钥。

开始之前

- 如果您已处于多情景模式下，请在系统执行空间中输入激活密钥。
- 某些永久许可证会在激活后要求重新加载 ASA。下表列出了要求重新加载的许可证。

表 *2:* 永久许可证重新加载要求

型号	要求重新加载的许可证操作
所有型号	降级加密许可证。

过程

步骤 1 将激活密钥应用于 ASA：

activation-key *key* [**activate** | **deactivate**]

示例：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

key 是包括五个元素的十六进制字符串，各元素之间以空格分隔。前导 0x 区分符是可选的；系统假定所有值都是十六进制值。

您可以安装一个永久密钥和 多个基于时间的密钥。如果输入新的永久密钥，则它会覆盖已安装的永久密钥。

activate 和 **deactivate** 关键字仅适用于基于时间的密钥。如果不输入任何值，则 **activate** 为默认值。您为给定功能激活的最后一个基于时间的密钥是活动密钥。要停用所有活动的基于时间的密钥，请输入 **deactivate** 关键字。如果您是第一次输入密钥，之后指定 **deactivate**，则在 ASA 上安装的密钥处于不活动状态。

步骤 2 （可能需要）。重新加载 ASA：

reload

输入新的激活密钥之后，某些永久许可证会要求您重新加载 ASA。如果您需要重新加载，将会看到以下消息：

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

相关主题

基于时间的许可证，第 2 页

配置共享许可证（Secure Client 3 及更早版本）

注释 Secure Client 4 及更高版本的许可不支持 ASA 上的共享许可证功能。 Secure Client 许可证是共享的，不再需要共享服务器或参与者许可证。

本节介绍如何配置共享许可服务器和参与者。

关于共享许可证

通过共享许可证，您可以购买大量的 Secure Client 高级会话，并且通过将一组 ASA 中的一个 ASA 配置为共享许可服务器，将剩余 ASA 配置为共享许可参与者，来根据需要在这组 ASA 之间共享会话。

关于共享许可服务器和参与者

以下步骤说明共享许可证的工作方式：

1. 确定哪一台ASA应充当共享许可服务器，然后使用该设备的序列号购买共享许可服务器许可证。

2. 确定哪些 ASA 应充当共享许可参与者（包括共享许可备用服务器），并使用每台设备的序列号获取每台设备的共享许可参与者许可证。
3. （可选）将另一台 ASA 指定为共享许可备用服务器。只能指定一台备用服务器。

注释 共享许可备用服务器仅需要参与者许可证。

4. 请在共享许可服务器上配置一个共享密钥；具有该共享密钥的所有参与者都可以使用共享许可证。
5. 将 ASA 配置为参与者时，它通过发送有关自身的信息（包括本地许可证和型号信息）向共享许可服务器注册。

注释 参与者需要能够通过 IP 网络与服务器通信；它不必在同一子网中。

6. 共享许可服务器会使用参与者应轮询服务器的频率的有关信息进行响应。
7. 当参与者用尽本地许可证的会话时，它会向共享许可服务器发出请求，从而获取更多会话（以 50 个会话为增量）。
8. 共享许可服务器使用共享许可证进行响应。参与者使用的会话总数不能超过平台型号的最大会话数。

注释 共享许可服务器也可以参与共享许可证池。它进行参与既不需要参与者许可证，也不需要服务器许可证。

   1. 如果在共享许可证池中没有为参与者留下足够多的会话，则服务器通过提供尽可能多的可用会话进行响应。
   2. 参与者会继续发送请求更多会话的刷新消息，直到服务器可以充分满足请求。

9. 当参与者的负载减少时，它会向服务器发送消息，以释放共享会话。

注释 ASA 在服务器和参与者之间使用 SSL 来加密所有通信。

参加者和服务器之间的通信问题

有关参与者和服务器之间的通信问题的信息，请参阅以下准则：

- 如果参与者在 3 倍刷新间隔后未能发送刷新信息，则服务器会将会话释放回共享许可证池。

- 如果参与者无法访问许可证服务器以发送刷新消息，则参与者可以继续使用其从服务器收到的共享许可证，最多可使用 24 小时。
- 如果在24小时后，参与者仍无法与许可证服务器通信，则参与者将释放共享许可证，即使其仍然需要会话也如此。参与者会保留已建立的现有连接，但无法接受超过许可证限制的新连接。
- 如果在24小时的时间到期之前且服务器使参与者会话到期之后，参与者与服务器重新连接，则参与者需要为会话发送新的请求；服务器通过可向该参与者发送尽可能多的会话进行响应。

关于共享许可备用服务器

共享许可备用服务器必须先成功向主共享许可服务器注册，然后才能承担备用角色。当其注册时，主共享许可服务器将与备用服务器同步服务器设置以及共享许可证信息，其中包括已注册参与者的列表以及当前的许可证使用情况。主服务器和备用服务器以10秒为间隔同步数据。在最初的同步之后，即使经过重新加载，备份服务器也能够成功履行备用职责。

当主服务器发生故障时，备用服务器会接管服务器操作。备用服务器可以连续运行最多30天，在此之后，备用服务器会停止向参与者发出会话，而且现有会话将会超时。请务必在此30天的时段内恢复主服务器。关键级别的系统日志消息会在 15 天时发送，并在 30 天时再次发送。

当主服务器恢复正常运行时，它将与备用服务器同步，然后接管服务器操作。

当备用服务器不处于主用状态时，它会充当主共享许可服务器的普通参与者。

注释 首次启动主共享许可服务器时，备用服务器仅可独立运行 5 天。运行限制将逐日延长，直至达到 30 天。此外，如果此后主服务器停止运行任意时长，则备用服务器的运行限制会逐日缩短。当主服务器恢复正常运行时，备用服务器的运行限制会开始再次逐日延长。例如，如果主服务器停止运行 20 天，在此期间备用服务器处于主用状态，则备用服务器的运行限制将仅剩余10天。备份服务器在继续充当非主用的备用服务器 20 天后，将“充值”至最长的 30 天运行限制。实施此“充值”功能是为了防止滥用共享许可证。

故障转移和共享许可证

本节介绍共享许可证如何与故障转移交互。

故障转移和共享许可证服务器

本节介绍主服务器和备用服务器如何与故障转移交互。由于共享许可服务器与ASA一样也会执行常规职责，包括执行VPN网关和防火墙等功能，则您可能需要为主和备用共享许可服务器配置故障转移，以提高可靠性。

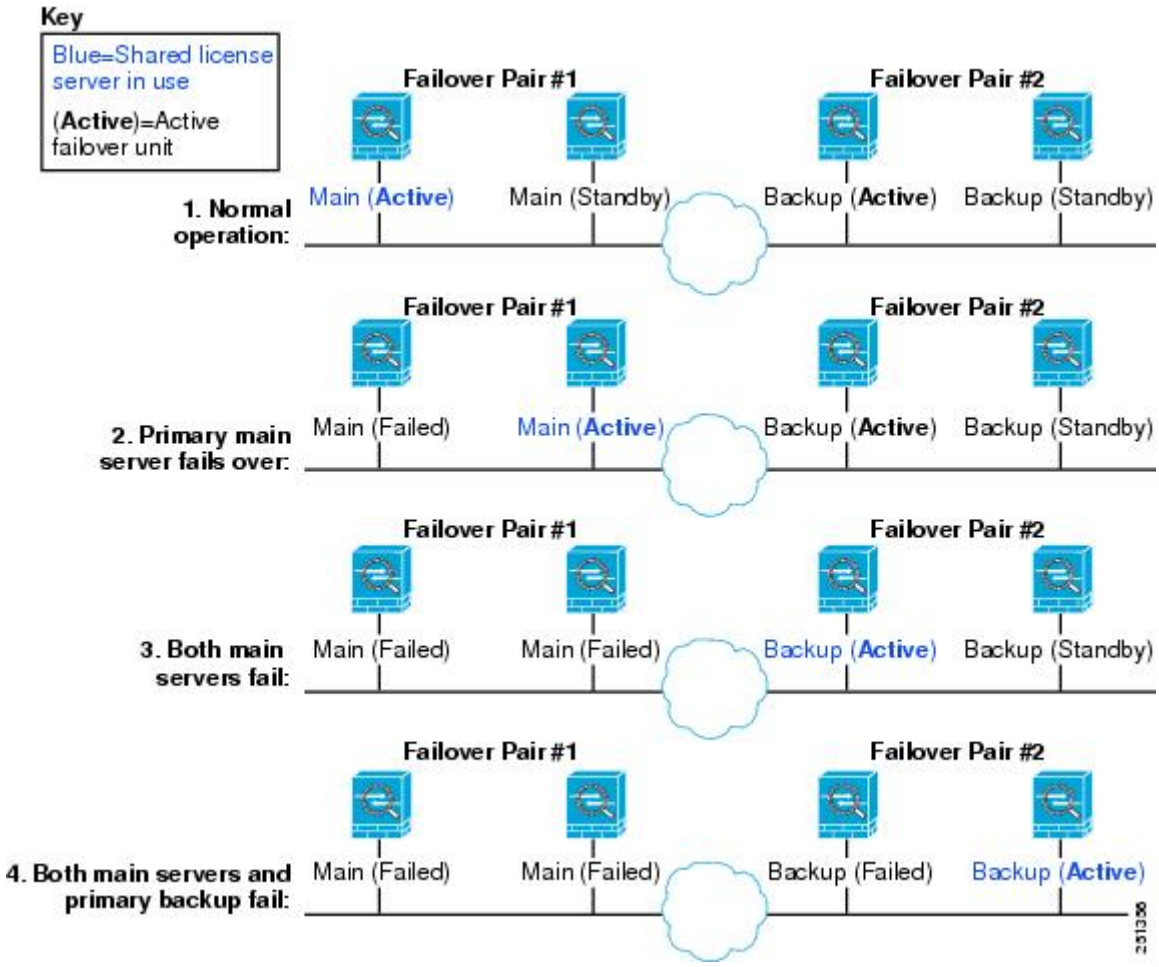
注释 备用服务器机制独立于故障转移，但与其兼容。

仅在单情景模式下支持共享许可证，因此不支持主用/主用故障转移。

对于主用/备用故障转移，主设备将充当主共享许可服务器，发生故障转移后，备用设备将充当主共享许可服务器。备用设备不会充当备用共享许可证服务器。相反，您可以视需要让另一对设备充当备用服务器。

例如，您具有包含 2 个故障转移对的网络。第 1 对包含主许可服务器。第 2 对包含备用服务器。第 1 对中的主设备发生故障时，备用设备会立即变为新的主许可服务器。绝不会使用第 2 对中的备用服务器。仅当第 1 对中的两台设备均发生故障时，第 2 对中的备用服务器才会用作共享许可服务器。如果第 1 对保持关闭，并且第 2 对中的主设备关闭，则第 2 对中的备用设备将用作共享许可服务器（请见下图）。

图 *6:* 故障转移和共享许可证服务器



辅助备用服务器与主备用服务器共享相同的运行限制；如果辅助设备变为主用设备，它会在主设备停止的位置继续倒计时。

相关主题

关于共享许可备用服务器，第 17 页

故障转移和共享许可证参与者

对于参与者对，两台设备均会使用单独的参与者 ID 向共享许可服务器注册。主用设备会将其参与者 ID 与备用设备同步。当备用设备切换到主用角色时，它会使用此 ID 生成转移请求。此转移请求用于将来自先前主用设备的共享会话移至新的主用设备。

最大参与者数

ASA 不限制共享许可证的参与者数量；但是，超大共享网络可能会潜在影响许可服务器的性能。在这种情况下，您可以增大参与者刷新之间的延迟，也可以创建两个共享网络。

配置共享许可服务器

此部分介绍如何将 ASA 配置为共享许可服务器。

开始之前

服务器必须具有共享许可服务器密钥。

过程

步骤 1 设置共享密钥：

license-server secret *secret*

示例：

```
ciscoasa(config)# license-server secret farscape
```

secret 是由 4 至 128 个 ASCII 字符组成的字符串。拥有此密钥的任何参与者都可以使用许可服务器。

步骤 2 （可选）设置刷新间隔：

license-server refresh-interval *seconds*

示例：

```
ciscoasa(config)# license-server refresh-interval 100
```

间隔介于 10 和 300 秒之间；此值会提供给参与者，用于设置其应与服务器通信的频率。默认值为 30 秒。

步骤 3 （可选）设置服务器侦听来自参与者的 SSL 连接的端口。

license-server port *port*

示例：

```
ciscoasa(config)# license-server port 40000
```

port 介于 1 和 65535 之间。默认值为 TCP 端口 50554。

步骤 4 （可选）确定备用服务器 IP 地址和序列号：

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

示例：

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

如果备用服务器属于某个故障转移对，请另外确定备用设备序列号。只能确定 1 台备用服务器及其可选的备用设备。

步骤 5 使此设备成为共享许可服务器：

license-server enable *interface_name*

示例：

```
ciscoasa(config)# license-server enable inside
```

指定参与者与服务器进行连接的接口。您可以为所需数量的接口重复此命令。

示例

以下示例设置共享密钥、更改刷新间隔和端口、配置备用服务器，并在内部接口和 dmz 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

配置共享许可备份服务器（可选）

本节介绍如何使共享许可参与者在主服务器发生故障时充当备用服务器。

开始之前

备用服务器必须具有共享许可参与者密钥。

过程

步骤 1 确定共享许可服务器 IP 地址和共享密钥：

license-server address *address* **secret** *secret* [**port** *port*]

示例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

如果更改服务器配置中的默认端口，请设置该端口，以便备用服务器能够匹配。

步骤 2 使此设备成为共享许可备用服务器：

license-server backup enable *interface_name*

示例：

```
ciscoasa(config)# license-server backup enable inside
```

指定参与者与服务器进行连接的接口。您可以为所需数量的接口重复此命令。

示例

以下示例确定许可服务器和共享密钥，并在内部接口和 dmz 接口上使此设备成为备用共享许可服务器：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

配置共享许可参与者

本部分配置共享许可参与者以与共享许可服务器进行通信。

开始之前

参与者必须具有共享许可参与者密钥。

过程

步骤 1 确定共享许可服务器 IP 地址和共享密钥：

license-server address *address* **secret** *secret* [**port** *port*]

示例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

如果更改服务器配置中的默认端口，请设置该端口，以便参与者能够匹配。

步骤 2 （可选）如果配置了备用服务器，请输入备用服务器地址：

license-server backup address *address*

示例：

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

示例

以下示例设置许可服务器 IP 地址和共享密钥，以及备用许可服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

每个型号支持的功能许可证

本节介绍适用于每个型号的许可证，以及有关这些许可证的重要说明。

每个型号的许可证

本节列出了适用于每个型号的功能许可证：

显示为斜体的项是可以替代基础许可证（或增强型安全许可证等）版本的独立可选许可证。可混合和匹配可选许可证。

注释 某些功能互不兼容。有关兼容性信息，请参阅单独的功能章节。

如果您拥有一个无负载加密型号，则无法支持下面的部分功能。有关不支持功能的列表，请参阅无负载加密型号，第 8 页。

有关许可证的详细信息，请参阅许可证说明，第 4 页。

ISA 3000 许可证功能

下表显示了 ISA 3000 已获许可的功能。

许可证	基础许可证		增强型安全许可证	
防火墙许可证				
僵尸网络流量过滤器	不支持		不支持	
并发防火墙连接数	20,000		50,000	
Carrier	不支持		不支持	
TLS 代理会话总数	160		160	
VPN 许可证				
Secure Client 对等体	禁用	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证：最多 *25* 个	禁用	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证：最多 *25* 个
其他 VPN 对等体数	10		50	
VPN对等体总数（包括所有类型）	25		50	
VPN 负载均衡	不支持		不支持	
通用许可证				
加密	基本 (DES)	可选许可证：强 *(3DES/AES)*	基本 (DES)	可选许可证：强 *(3DES/AES)*
故障转移	不支持		主用/备用	
安全情景	不支持		不支持	
集群	不支持		不支持	
最大 VLAN 数量	5		25	

监控 PAK 许可证

本节介绍如何查看许可证信息。

查看您当前的许可证

此部分介绍如何查看您的当前许可证，以及与基于时间的激活密钥对应的许可证的剩余时间。

开始之前

如果您拥有的是无负载加密型号，则在查看许可证时，将不会列出VPN许可证和统一通信许可证。有关详细信息，请参阅无负载加密型号，第 8 页。

过程

显示永久许可证、活动的基于时间的许可证以及运行许可证（包括永久许可证和活动的基于时间的许可证）：

show activation-key [**detail**]

detail 关键字还显示非活动的基于时间的许可证。

对于故障转移或集群设备，该命令还显示“集群”许可证，该许可证包括所有设备的密钥。

示例

示例 1：独立设备运行 show activation-key 命令时的输出

以下是独立设备运行 **show activation-key** 命令时的样本输出，其中显示运行许可证（包括永久许可证和活动的基于时间的许可证）以及每个活动的基于时间的许可证：

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.
```

```
The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

示例 2：独立设备运行 show activation-key detail 时的输出

以下是独立设备运行 **show activation-key detail** 命令时的样本输出，其中显示运行许可证（合并的永久许可证和基于时间的许可证），以及永久许可证和每个已安装的基于时间的许可证（活动和非活动）：

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              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        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              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       39 days
Intercompany Media Engine      : Disabled      perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

示例 3：故障转移对中的主设备运行 show activation-key detail 时的输出

以下是主故障转移设备运行 **show activation-key detail** 命令时的样本输出，其中显示：

- 主设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 主设备永久许可证。
- 主设备安装的基于时间的许可证（活动和非活动）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            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        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
```

```
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Enabled        perpetual
Security Contexts             : 12             perpetual
GTP/GPRS                      : Enabled        perpetual
AnyConnect Premium Peers      : 4            perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 750            perpetual
Total VPN Peers                 : 750            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       : 4              perpetual
Total UC Proxy Sessions       : 4              perpetual
Botnet Traffic Filter         : Enabled        33 days
Intercompany Media Engine     : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces   : Unlimited      perpetual
Maximum VLANs                 : 150            perpetual
Inside Hosts                  : Unlimited      perpetual
Failover                      : Active/Active  perpetual
VPN-DES                       : Enabled        perpetual
VPN-3DES-AES                  : Disabled       perpetual
Security Contexts             : 2              perpetual
GTP/GPRS                      : Disabled       perpetual
AnyConnect Premium Peers        : 2              perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 750            perpetual
Total VPN Peers                 : 750            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         : Disabled       perpetual
Intercompany Media Engine     : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter          : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts              : 2          7 days
AnyConnect Premium Peers                  : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions        : 100        14 days
```

示例 4：故障转移对中的辅助设备运行 show activation-key detail 时的输出

以下是辅助故障转移设备运行 **show activation-key detail** 命令时的样本输出，其中显示：

- 辅助设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 辅助设备永久许可证。
- 辅助设备安装的基于时间的许可证（活动和非活动）。此设备没有任何基于时间的许可证，因此在此样本输出中不会显示任何内容。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            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          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            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        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
```

```
This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            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          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

示例 5：故障转移对中的 ASA 服务模块的主设备运行 show activation-key 时的输出

以下是主故障转移设备运行 **show activation-key** 命令时的样本输出，其中显示：

- 主设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 主设备安装的基于时间的许可证（活动和非活动）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
```

```
Failover                         : Active/Active  perpetual
DES                              : Enabled        perpetual
3DES-AES                         : Enabled        perpetual
Security Contexts                : 50 perpetual
GTP/GPRS                         : Enabled        perpetual
Botnet Traffic Filter            : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

示例 6：故障转移对中的 ASA 服务模块的辅助设备运行 show activation-key 时的输出

以下是辅助故障转移设备运行 **show activation-key** 命令时的样本输出，其中显示：

- 辅助设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 辅助设备安装的基于时间的许可证（活动和非活动）。此设备没有任何基于时间的许可证，因此在此样本输出中不会显示任何内容。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces               : 1024           perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
DES                              : Enabled        perpetual
3DES-AES                         : Enabled        perpetual
Security Contexts                : 25             perpetual
GTP/GPRS                         : Disabled       perpetual
Botnet Traffic Filter            : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces               : 1024           perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
DES                              : Enabled        perpetual
3DES-AES                         : Enabled        perpetual
Security Contexts                : 50 perpetual
GTP/GPRS                         : Enabled perpetual
Botnet Traffic Filter            : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

示例 7：集群运行 show activation-key 时的输出

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 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 : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 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 : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 The flash permanent activation key is the SAME as the running permanent key.
```

监控共享许可证

要监控共享许可证，请输入以下命令之一。

- **show shared license** [**detail** | **client** [*hostname*] | **backup**]

  显示共享许可证统计信息。可选关键字仅适用于许可服务器：**detail** 关键字用于显示每个参与者的统计信息。要将显示内容限制为一个参与者的相关信息，请使用 **client** 关键字。**backup** 关键字用于显示有关备用服务器的信息。

  要清除共享许可证统计信息，请输入 **clear shared license** 命令。

  以下是许可证参与者上 **show shared license** 命令的样本输出：

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

  以下是许可证服务器上 **show shared license detail** 命令的样本输出：

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:
```

```
  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

- **show activation-key**

  显示 ASA 上安装的许可证。**show version** 命令也可用于显示许可证信息。

- **show vpn-sessiondb**

  显示有关 VPN 会话的许可证信息。

PAK 许可证的历史

功能名称	平台版本	说明
增加了连接数和 VLAN 数量	7.0(5)	提高了以下限制： • ASA5510 基础许可证连接数从 32000 增加到 50000；VLAN 数从 0 增加到 10。 • ASA5510 基础许可证连接数从 64000 增加到 130000；VLAN 数从 10 增加到 25。 • ASA5520 连接数从 130000 增加到 280000；VLAN 数从 25 增加到 100。 • ASA5540 连接数从 280000 增加到 400000；VLAN 数从 100 增加到 200。
SSL VPN 许可证	7.1(1)	引入了 SSL VPN 许可证。
增加了 SSL VPN 许可证数量	7.2(1)	为 ASA 5550 和更高版本引入了 5000 用户 SSL VPN 许可证。
ASA 5510 上的基础许可证增加了接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。

功能名称	平台版本	说明
增加了 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能；1 个故障转移；1 个限用于备用接口）增加到 20 个全功能接口。此外，中继端口数量也从 1 增加到 8。现在有 20 个全功能接口，您不需要使用 backup interface 命令禁用备用 ISP 接口的功能；您可以为其使用全功能接口。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有所增加：ASA 5510（对于基础许可证，从 10 增加到 50；对于增强型安全许可证，从 25 增加到 100）、ASA 5520（从 100 增加到 150）和 ASA 5550（从 200 增加到 250）。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	具有增强型安全许可证的 ASA 5510 现在在 Ethernet 0/0 和 0/1 端口上支持千兆以太网 (1000 Mbps)。在基础许可证中，它们将继续用作快速以太网 (100 Mbps) 端口。对于两种许可证，Ethernet 0/2、0/3 和 0/4 仍为快速以太网端口。 **注释** 接口名称仍为 Ethernet 0/0 和 Ethernet 0/1。 使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。
高级终端评估许可证	8.0(2)	引入了高级终端评估许可证。作为 Cisco AnyConnect 或无客户端 SSL VPN 连接完成的一个条件，远程计算机将对一系列规模大幅扩展的防病毒软件和反间谍软件应用、防火墙、操作系统以及相关更新进行扫描。它还会扫描您指定的所有注册表项、文件名和进程名称，它会将扫描结果发送至 ASA。ASA 使用用户登录凭证和计算机扫描结果来指定动态访问策略 (DAP)。 借助高级终端评估许可证，您可以进行相关配置，以尝试对不合规计算机进行更新（使其符合版本要求），从而增强主机扫描。 思科可通过独立于思科安全桌面的软件包，对主机扫描所支持的应用和版本的列表进行及时更新。
ASA 5510 的 VPN 负载均衡	8.0(2)	ASA 5510 增强型安全许可证现在支持 VPN 负载均衡。
适用于移动设备的 AnyConnect 许可证	8.0(3)	引入了适用于移动设备的 AnyConnect 许可证。通过它，Windows 移动设备可以使用 Secure Client连接至 ASA。
基于时间的许可证	8.0(4)/8.1(2)	引入了对基于时间的许可证的支持。
增加了 ASA 5580 的 VLAN 数量	8.1(2)	在 ASA 5580 上支持的 VLAN 数量从 100 增加到 250。

功能名称	平台版本	说明
统一通信代理会话许可证	8.0(4)	引入了 UC 代理会话许可证。电话代理、状态联合代理和加密语音检测应用会在其连接中使用 TLS 代理会话。根据 UC 许可证限制对每个 TLS 代理会话进行计数。所有这些应用都在 UC 代理伞状结构下获得许可，并且可以混合搭配使用。 此功能在版本 8.1 中不可用。
僵尸网络流量过滤器许可证	8.2(1)	引入了僵尸网络流量过滤器许可证。僵尸网络流量过滤器可以跟踪通向已知不良域名和 IP 地址的连接，从而防御恶意软件网络活动。
AnyConnect 基础版许可证	8.2(1)	引入了 AnyConnect 基础版许可证。此许可证支持 AnyConnect VPN 客户端访问 ASA。此许可证不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect 高级版许可证而不是 AnyConnect 基础版许可证。 **注释** 借助 AnyConnect 基础版许可证，VPN 用户可以使用 Web 浏览器来进行登录，然后下载并启动 (WebLaunch) Secure Client。 Secure Client 软件提供一系列相同的客户端功能，无论是通过此许可证还是通过 AnyConnect 高级版许可证启用。 AnyConnect 基础版许可证不能与给定 ASA 上的以下许可证同时处于活动状态：AnyConnect 高级版许可证（所有类型）或高级终端评估许可证。但您可以在同一网络内的不同 ASA 上运行 AnyConnect 基础版和 AnyConnect 高级版许可证。 默认情况下，ASA 使用 AnyConnect 基础版许可证，但您可以通过如下方式将其禁用，以使用其他许可证：使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令。
SSL VPN 许可证更改为 AnyConnect 高级版 SSL VPN 版本许可证	8.2(1)	SSL VPN 许可证的名称更改为 AnyConnect 高级版 SSL VPN 版本许可证。
SSL VPN 共享许可证	8.2(1)	引入了 SSL VPN 共享许可证。多个 ASA 可以按需共享一个 SSL VPN 会话池。
移动代理应用不再需要统一通信代理许可证	8.2(2)	移动代理不再需要 UC 代理许可证。
10 GE I/O 许可证（用于带 SSP-20 的 ASA 5585-X）	8.2(3)	引入了 10 GE I/O 许可证（用于带 SSP-20 的 ASA 5585-X），以便在光纤端口上支持 10 千兆以太网速度。默认情况下，SSP-60 支持 10 千兆以太网速度。 **注释** 在 8.3(x) 版本中不支持 ASA 5585-X。

功能名称	平台版本	说明
10 GE I/O 许可证（用于带 SSP-10 的 ASA 5585-X）	8.2(4)	引入了 10 GE I/O 许可证（用于带 SSP-10 的 ASA 5585-X），以便在光纤端口上支持 10 千兆以太网速度。默认情况下，SSP-40 支持 10 千兆以太网速度。 **注释** 在 8.3(x) 版本中不支持 ASA 5585-X。
不相同的故障转移许可证	8.3(1)	不再要求每个设备上的故障转移许可证相同。来自主设备和辅助设备的合并许可证是同时用于这两种设备的许可证。 修改了以下命令：**show activation-key** 和 **show version**。
可堆叠的基于时间的许可证	8.3(1)	基于时间的许可证现在可以堆叠。在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，许可证没有到期尤为重要。ASA 允许堆叠基于时间的许可证，从而让您不必担忧许可证到期或由于提前安装了新许可证而损害许可证上的时间。
公司间媒体引擎许可证	8.3(1)	引入了 IME 许可证。
多个基于时间的许可证同时处于活动状态	8.3(1)	您现在可以安装多个基于时间的许可证，每个功能一次只能有一个许可证处于活动状态。 修改了以下命令：**show activation-key** 和 **show version**。
基于时间的许可证的独立激活和停用。	8.3(1)	您现在可以使用一个命令来激活或停用基于时间的许可证。 修改了以下命令：**activation-key** [**activate** | **deactivate**]。
AnyConnect 高级版 SSL VPN 版本许可证更改为 AnyConnect 高级版 SSL VPN 许可证	8.3(1)	AnyConnect 高级版 SSL VPN 版本许可证的名称更改为 AnyConnect 高级版 SSL VPN 许可证。
用于出口的无负载加密映像	8.3(2)	如果您在 ASA 5505 至 5550 上安装无负载加密软件，则会禁用统一通信、强加密 VPN 和强加密管理协议。 **注释** 此特殊映像仅在 8.3(x) 中受支持；要想在 8.4(1) 及更高版本中支持无负载加密，您需要购买 ASA 的特殊硬件版本。
增加了 ASA 5550、5580 和 5585-X 的情景数	8.4(1)	对于带 SSP-10 的 ASA 5550 和 ASA 5585-X，最大情景数从 50 增加到 100。对于带 SSP-20 和更高版本的 ASA 5580 和 5585-X，最大数量从 50 增加到 250。
增加了 ASA 5580 和 5585-X 的 VLAN 数量	8.4(1)	对于 ASA 5580 和 5585-X，最大 VLAN 数量从 250 增加到 1024。

功能名称	平台版本	说明
增加了 ASA 5580 和 5585-X 的连接数	8.4(1)	提高了防火墙连接限制： • ASA 5580-20 - 1,000,000 至 2,000,000。 • ASA 5580-40 - 2,000,000 至 4,000,000。 • 带 SSP-10 的 ASA 5585-X：750,000 至 1,000,000。 • 带 SSP-20 的 ASA 5585-X：1,000,000 至 2,000,000。 • 带 SSP-40 的 ASA 5585-X：2,000,000 至 4,000,000。 • 带 SSP-60 的 ASA 5585-X：2,000,000 至 10,000,000。
AnyConnect 高级版 SSL VPN 许可证更改为 AnyConnect 高级版许可证	8.4(1)	AnyConnect 高级版 SSL VPN 许可证的名称更改为 AnyConnect 高级版许可证。许可证信息显示从“SSL VPN Peers”更改为“AnyConnect Premium Peers”。
增加了 ASA 5580 的 AnyConnect VPN 会话数	8.4(1)	AnyConnect VPN 会话限制从 5,000 增加到 10,000。
增加了 ASA 5580 的其他 VPN 会话数	8.4(1)	其他 VPN 会话数限值从 5,000 增加到 10,000。
使用 IKEv2 的 IPsec 远程访问 VPN	8.4(1)	向 AnyConnect 基础版和 AnyConnect 高级版许可证中添加了使用 IKEv2 的 IPsec 远程访问 VPN。 **注释** ASA 上对 IKEv2 的支持存在以下限制： 我们当前不支持重复的安全关联。 IKEv2 站点间会话已添加到其他 VPN 许可证（以前为 IPsec VPN）。其他 VPN 许可证包含在基础许可证中。
用于出口的无负载加密硬件	8.4(1)	对于支持无负载加密的型号（例如 ASA 5585-X），ASA 软件将禁用统一通信和 VPN 功能，从而使 ASA 可以出口至某些国家/地区。
适用于 SSP-20 和 SSP-40 的双 SSP	8.4(2)	对于 SSP-40 和 SSP-60，您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP（例如，不支持混用 SSP-40 和 SSP-60）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障转移对。当在机箱中使用两个 SSP 时不支持 VPN；但请注意，VPN 并没有被禁用。
ASA 5512-X 至 ASA 5555-X 的 IPS 模块许可证	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 上的 IPS SSP 软件模块需要 IPS 模块许可证。
ASA 5580 和 5585-X 的集群许可证	9.0(1)	为 ASA 5580 和 5585-X 添加了集群许可证。
ASASM 上支持 VPN	9.0(1)	ASASM 现在支持所有 VPN 功能。

功能名称	平台版本	说明
ASASM 上支持统一通信	9.0(1)	ASASM 现在支持所有统一通信功能。
SSP-10 和 SSP-20 的 ASA 5585-X 双 SSP 支持（SSP-40 和 SSP-60 除外）；双 SSP 的 VPN 支持	9.0(1)	ASA 5585-X 现在支持所有 SSP 型号使用双 SSP（在同一机箱中，您可以使用两个相同级别的 SSP）。使用双 SSP 时，现在支持 VPN。
ASA 5500-X 对集群的支持	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 现在支持由 2 台设备组成的集群。默认情况下，在基础许可证中支持两台设备的集群；对于 ASA 5512-X，您需要增强型安全许可证。
对 ASA 5585-X 支持 16 个集群成员	9.2(1)	ASA 5585-X 现在支持由 16 台设备组成的集群。
引入了 ASAv4 和 ASAv30 标准版和高级版型号许可证	9.2(1)	ASAv 带有一种简单的许可方案：标准版和高级版级别的 ASAv4 和 ASAv30 永久许可证。无可用的附加许可证。

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。