ASA 的许可证管理

通过思科智能软件许可，您可以集中购买和管理许可证池。您可以轻松部署或停用设备，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 本节仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。

关于智能软件许可

本部分介绍智能软件许可的工作原理。

注释 本节仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。

适用于 ASA 的智能软件许可

对于 Firepower 4100/9300 机箱上的 ASA 应用，智能软件许可配置分为两部分，分别在 Firepower 4100/9300 机箱管理引擎和应用中进行。

- Firepower 4100/9300 机箱- 所有智能软件许可基础设施均在管理引擎中配置，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 - 配置应用中的所有许可证授权。

注释 Firepower 4100/9300 安全设备上不支持思科传输网关。

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且无法注册到许可证颁发机构，可以配置离线许可。

永久许可证预留

如果您的设备出于安全原因而无法访问互联网，您可以选择为每个ASA请求永久许可证。永久许可证不需要定期访问许可证颁发机构。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。

您可以获取启用所有功能的许可证：具有最多安全环境的标准层级许可证和运营商许可证。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。

卫星服务器

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。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。

一旦下载并部署该卫星应用之后，即可在不使用互联网将数据发送到思科SSM的情况下执行以下功能：

- 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，请参阅智能账户管理器卫星上的智能软件管理器卫星安装和配置指南。

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。

仅 Firepower 4100/9300 机箱会注册为设备，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

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 您无法获得针对强密码 (3DES/AES) 的评估许可证；仅永久许可证支持此授权。

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。当部署每个机箱或注册现有机箱时，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。

在完成部署后或在现有机箱上手动配置这些参数后启动时，该机箱会向思科许可证颁发机构进行注册。当机箱向令牌注册时，许可证颁发机构会颁发一张ID证书，用于机箱与许可证颁发机构之间的通信。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。

Firepower 4100/9300 机箱 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。

注释 如果您的设备在一年内无法与许可证颁发机构通信，则设备将进入未注册状态，但不会丧失任何以前启用的强加密功能。

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。

要验证您的账户是否处于或接近不合规状态，必须将 Firepower 4100/9300 机箱当前正在使用的授权与智能账户中的授权进行比较。

在不合规状态下，无法更改需要特殊许可证的功能配置，但操作不受影响。例如，基于标准许可证限制的现有环境可以继续运行，您可以修改它们的配置，但无法添加新环境。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件位于指定许可证颁发机构 URL 的 FXOS 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 Firepower 4100/9300 安全设备上不支持思科传输网关。

思科成功网络

思科成功网络是一项用户启用的云服务。启用思科成功网络时，Firepower 4100/9300 机箱与思科云之间会建立安全连接以传输使用情况信息和统计信息。流传输遥测数据可以提供一种机制，用于从 ASA 选择感兴趣的数据，并使用结构化格式将其传输到远程管理站，以便执行以下任务：

- 向您告知在网络中可用来改进产品效果的未使用功能。
- 向您告知可能适用于您的产品的其他技术支持服务和监控。
- 帮助思科改善我们的产品

将 Firepower 4100/9300注册到思科智能软件管理器时，可启用思科成功网络。请参阅向许可证颁发机构注册 Firepower 安全设备，第 17 页。

仅当满足以下所有条件时，才可以注册 Cisco Success Network：

- 已注册智能软件许可证。
- 已禁用智能许可证卫星模式。
- 已禁用永久许可证。

当您注册 Cisco Success Network 后，机箱总是会建立并维护安全的连接。您可以通过禁用思科成功网络随时关闭此连接，这样会将设备与思科成功网络云断开。

您可以在**系统** > **许可** > **Cisco Success Network** 页面上查看当前的 Cisco Success Network 注册状态，还可以更改注册状态。请参阅更改 Cisco Success Network 注册，第 18 页。

思科成功网络遥测数据

Cisco Success Network 允许机箱每 24 小时向 Cisco Success Network 云端流传输一次配置和运行状态信息。收集和监控的数据包括：

- **注册设备信息** - Firepower 4100/9300 机箱 型号名称、产品标识符、序列号、UUID、系统正常运行时间和智能许可信息。请参阅已注册设备数据，第 6 页。
- **软件信息** - 在 Firepower 4100/9300 机箱 上运行的软件的类型和版本号。请参阅软件版本数据，第 6 页。
- **ASA 设备信息** - 与 Firepower 4100/9300 的 安全模块/引擎 上运行的 ASA 设备相关的信息。请注意，对于 Firepower 4100 系列，仅包含有关单个 ASA 设备的信息。ASA 设备信息包括每个设备的在用智能许可证、设备型号、序列号和软件版本。请参阅ASA 设备数据，第 7 页。
  - **性能信息** - ASA 设备的系统正常运行时间、CPU 使用率、内存使用率、磁盘空间使用情况和带宽使用信息。请参阅性能数据，第 7 页。

- **使用信息** - 功能状态、集群、故障切换和登录信息：
  - **功能状态** - 您已配置或默认启用的已启用 ASA 功能的列表。
  - **集群信息** - 如果 ASA 设备处于集群模式，则包括集群信息。如果 ASA 设备未处于集群模式，则不会显示此信息。集群信息包括ASA设备的集群组名称、集群接口模式、设备名称和状态。对于同一集群中的其他对等设备，这些信息包括名称、状态和序列号。
  - **故障切换信息** - 如果 ASA 处于故障切换模式，则包括故障切换信息。如果 ASA 未处于故障切换模式，则不会显示此信息。故障切换信息包括ASA的角色和状态，以及对等 ASA 设备的角色、状态和序列号。
  - **登录历史记录** - ASA 设备上的用户登录频率、登录时间和最近成功登录的日期戳。但是，登录历史记录不包括用户登录名、凭证或任何其他个人信息。

有关详细信息，请参阅使用数据，第 8 页。

已注册设备数据

在 Cisco Success Network 中注册 Firepower 4100/9300 机箱 后，选定的机箱相关遥测数据将流传输到思科云。下表说明所收集和监控的数据。

表 *1:* 已注册设备遥测数据

数据点	示例值
设备型号	思科 Firepower FP9300 安全设备
序列号	GMX1135L01K
智能许可证 PIID	752107e9-e473-4916-8566-e26d0c4a5bd9
智能许可证虚拟帐户名称	FXOS-general
系统运行时间	32115
UDI 产品标识符	FPR-C9300-AC

软件版本数据

Cisco Success Network 会收集与机箱相关的软件信息，包括类型和软件版本。下表说明所收集和监控的软件信息。

表 *2:* 软件版本遥测数据

数据点	示例值
类型	package_version
版本	2.7(1.52)

ASA 设备数据

Cisco Success Network 会收集上与 Firepower 4100/9300 的 安全模块/引擎 上运行的 ASA 设备相关的信息。下表说明所收集和监控的 ASA 设备相关信息。

表 *3: ASA* 设备遥测数据

数据点	示例值
ASA 设备 PID	FPR9K-SM-36
ASA 设备型号	思科自适应安全设备
ASA 设备序列号	XDQ311841WA
部署类型（本地或容器）	原生型
安全上下文模式（单或多）	单值

ASA 软件版本	{
	type: "asa_version",
	ersion: "9.13.1.5"
	}

设备管理器版本	{
	type: "device_mgr_version",
	version: "7.10.1"
	}

正在使用的已激活智能许可证	{
	"type": "Strong encryption",
	"tag":
	"regid.2016-05.com.cisco.ASA-GEN-STRONG-ENCRYPTION,
	5.7_982308k4-74w2-5f38-64na-707q99g10cce",
	"count": 1
	}

性能数据

Cisco Success Network 会收集 ASA 设备的性能特定信息。这些信息包括系统正常运行时间、CPU 使用率、内存使用率、磁盘空间使用情况和带宽使用信息。

- **CPU 使用率** - 过去五分钟的 CPU 使用信息
- **内存使用率** - 系统的可用、已用及总内存
- **磁盘使用情况** - 可用、已用及总磁盘空间信息
- **系统正常运行时间** - 系统正常运行时间信息
- **带宽使用** - 系统带宽使用情况；从所有 nameif 接口汇聚

  这会显示自系统启动时间以来已接收和传输的数据包（或字节）的统计信息。

下表说明所收集和监控的数据。

表 *4:* 性能遥测数据

数据点	示例值

过去五分钟的系统 CPU 使用率	{
	“fiveSecondsPercentage”:0.2000000,
	“oneMinutePercentage”: 0,
	“fiveMinutesPercentage”: 0
	
	}

系统内存使用率	{
	“freeMemoryInBytes”:225854966384,
	“usedMemoryInBytes”: 17798281616,
	“totalMemoryInBytes”:243653248000
	
	}

系统磁盘使用情况	{
	"freeGB": 21.237285,
	"usedGB": 0.238805,
	"totalGB": 21.476090
	
	}

系统运行时间	99700000

系统带宽使用情况	{
	"receivedPktsPerSec": 3,
	"receivedBytesPerSec": 212,
	"transmittedPktsPerSec": 3,
	"transmittedBytesPerSec": 399
	}

使用数据

Cisco Success Network 会收集机箱的 安全模块/引擎 上运行的 ASA 设备的功能状态、集群、故障切换和登录信息。下表说明所收集和监控的 ASA 设备使用数据。

表 *5:* 使用情况遥测数据

数据点	示例值

功能状态	[{
	“name”: “cluster”,
	“status”: “enabled”
	},
	{
	“name”: “webvpn”,
	“status”: “enabled”
	},
	{
	“name”: “logging-buffered”,
	“status”: “debugging”
	}]

数据点	示例值

集群信息	<pre>{
	"clusterGroupName": "asa-cluster",
	"interfaceMode": "spanned",
	"unitName": "unit-3-3",
	"unitState": "SLAVE",
	"otherMembers": {
	"items": [
	{
	"memberName": "unit-2-1",
	"memberState": "MASTER",
	
	"memberSerialNum": "DAK391674E"
	}
	]
	}
	
	}</pre>

故障切换信息	<pre>{
	myRole: “Primary”,
	peerRole: “Secondary”,
	myState: “active”,
	peerState: “standby”,
	peerSerialNum:
	“DAK39162B”
	}</pre>

登录历史	<pre>{
	"loginTimes": "1 times in last 1 days",
	"lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
	}</pre>

遥测示例文件

Firepower 4100/9300 机箱汇聚从已启用遥测的所有 ASA 设备接收的数据，并在将数据发送到思科云之前，与机箱特定信息和其他字段一起位于线上。如果没有具有遥测数据的应用程序，则仍将遥测与机箱信息一起发送到思科云。

以下是 Cisco Success Network 遥测文件的一个示例，其中包含发送到思科云的 Firepower 9300 上两台 ASA 设备的信息。


```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json",
    "msgID": "2227"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1560868270055,
    "FXOS": {
      "FXOSdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "HNY4475P01K",
        "smartLicenseProductInstanceIdentifier": "413509m0-f952-5822-7492-r62c0a5h4gf4",
```

```
    "smartLicenseVirtualAccountName": "FXOS-general",
    "systemUptime": 32115,
    "udiProductIdentifier": "FPR-C9300-AC"
  },
  "versions": {
    "items": [
      {
        "type": "package_version",
        "version": "2.7(1.52)"
      }
    ]
  }
},
"asaDevices": {
  "items": [
    {
      "CPUUsage": {
        "fiveMinutesPercentage": 0,
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0
      },
      "bandwidthUsage": {
        "receivedBytesPerSec": 1,
        "receivedPktsPerSec": 0,
        "transmittedBytesPerSec": 1,
        "transmittedPktsPerSec": 0
      },
      "deviceInfo": {
        "deploymentType": "Native",
        "deviceModel": "Cisco Adaptive Security Appliance",
        "securityContextMode": "Single",
        "serialNumber": "ADG2158508T",
        "systemUptime": 31084,
        "udiProductIdentifier": "FPR9K-SM-24"
      },
      "diskUsage": {
        "freeGB": 19.781810760498047,
        "totalGB": 20.0009765625,
        "usedGB": 0.21916580200195312
      },
      "featureStatus": {
        "items": [
          {
            "name": "aaa-proxy-limit",
            "status": "enabled"
          },
          {
            "name": "firewall_user_authentication",
            "status": "enabled"
          },
          {
            "name": "IKEv2 fragmentation",
            "status": "enabled"
          },
          {
            "name": "inspection-dns",
            "status": "enabled"
          },
          {
            "name": "inspection-esmtp",
            "status": "enabled"
          },
          {
            "name": "inspection-ftp",
```

```
    "status": "enabled"
  },
  {
    "name": "inspection-hs232",
    "status": "enabled"
  },
  {
    "name": "inspection-netbios",
    "status": "enabled"
  },
  {
    "name": "inspection-rsh",
    "status": "enabled"
  },
  {
    "name": "inspection-rtsp",
    "status": "enabled"
  },
  {
    "name": "inspection-sip",
    "status": "enabled"
  },
  {
    "name": "inspection-skinny",
    "status": "enabled"
  },
  {
    "name": "inspection-snmp",
    "status": "enabled"
  },
  {
    "name": "inspection-sqlnet",
    "status": "enabled"
  },
  {
    "name": "inspection-sunrpc",
    "status": "enabled"
  },
  {
    "name": "inspection-tftp",
    "status": "enabled"
  },
  {
    "name": "inspection-xdmcp",
    "status": "enabled"
  },
  {
    "name": "management-mode",
    "status": "normal"
  },
  {
    "name": "mobike",
    "status": "enabled"
  },
  {
    "name": "ntp",
    "status": "enabled"
  },
  {
    "name": "sctp-engine",
    "status": "enabled"
  },
  {
    "name": "smart-licensing",
```

```
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
  "licenseActivated": {
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:18 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226031548496,
    "totalMemoryInBytes": 241583656960,
    "usedMemoryInBytes": 15552108464
  },
  "versions": {
    "items": [
      {
        "type": "asa_version",
        "version": "9.13(1)248"
      },
      {
        "type": "device_mgr_version",
        "version": "7.13(1)31"
      }
    ]
  }
},
{
  "CPUUsage": {
    "fiveMinutesPercentage": 0,
    "fiveSecondsPercentage": 0,
    "oneMinutePercentage": 0
  },
  "bandwidthUsage": {
    "receivedBytesPerSec": 1,
    "receivedPktsPerSec": 0,
    "transmittedBytesPerSec": 1,
    "transmittedPktsPerSec": 0
  },
  "deviceInfo": {
    "deploymentType": "Native",
    "deviceModel": "Cisco Adaptive Security Appliance",
    "securityContextMode": "Single",
    "serialNumber": "RFL21764S1D",
    "systemUptime": 31083,
    "udiProductIdentifier": "FPR9K-SM-24"
  },
  "diskUsage": {
    "freeGB": 19.781543731689453,
    "totalGB": 20.0009765625,
```

```
  "usedGB": 0.21943283081054688
},
"featureStatus": {
  "items": [
    {
      "name": "aaa-proxy-limit",
      "status": "enabled"
    },
    {
      "name": "call-home",
      "status": "enabled"
    },
    {
      "name": "crypto-ca-trustpoint-id-usage-ssl-ipsec",
      "status": "enabled"
    },
    {
      "name": "firewall_user_authentication",
      "status": "enabled"
    },
    {
      "name": "IKEv2 fragmentation",
      "status": "enabled"
    },
    {
      "name": "inspection-dns",
      "status": "enabled"
    },
    {
      "name": "inspection-esmtp",
      "status": "enabled"
    },
    {
      "name": "inspection-ftp",
      "status": "enabled"
    },
    {
      "name": "inspection-hs232",
      "status": "enabled"
    },
    {
      "name": "inspection-netbios",
      "status": "enabled"
    },
    {
      "name": "inspection-rsh",
      "status": "enabled"
    },
    {
      "name": "inspection-rtsp",
      "status": "enabled"
    },
    {
      "name": "inspection-sip",
      "status": "enabled"
    },
    {
      "name": "inspection-skinny",
      "status": "enabled"
    },
    {
      "name": "inspection-snmp",
      "status": "enabled"
    },
```

```
      {
        "name": "inspection-sqlnet",
        "status": "enabled"
      },
      {
        "name": "inspection-sunrpc",
        "status": "enabled"
      },
      {
        "name": "inspection-tftp",
        "status": "enabled"
      },
      {
        "name": "inspection-xdmcp",
        "status": "enabled"
      },
      {
        "name": "management-mode",
        "status": "normal"
      },
      {
        "name": "mobike",
        "status": "enabled"
      },
      {
        "name": "ntp",
        "status": "enabled"
      },
      {
        "name": "sctp-engine",
        "status": "enabled"
      },
      {
        "name": "smart-licensing",
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
  "licenseActivated": {
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:16 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226028740080,
    "totalMemoryInBytes": 241581195264,
    "usedMemoryInBytes": 15552455184
  },
  "versions": {
    "items": [
```

```
            {
              "type": "asa_version",
              "version": "9.13(1)248"
            },
            {
              "type": "device_mgr_version",
              "version": "7.13(1)31"
            }
          ]
        }
      }
    ]
  }
 }
}
```


智能软件许可必备条件

- 请注意，本章仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。
- 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。
- 通过思科商务工作空间购买 1 个或多个许可证。在主页上，通过**查找产品和解决方案 (Find Products and Solutions)** 搜索字段搜索您的平台。有些许可证是免费的，但您仍需要将它们添加到智能软件许可账户。
- 确保可从机箱访问互联网或访问 HTTP 代理，以使机箱能够访问许可证颁发机构。
- 配置 DNS 服务器，以使机箱能够解析许可证颁发机构的名称。
- 设置机箱的时间。
- 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。

智能软件许可准则

ASA 故障切换和群集指南

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。辅助设备不会产生额外成本。 对于预留永久许可证，必须为每个机箱购买单独的许可证。

智能软件许可的默认设置

Firepower 4100/9300 机箱默认配置包括名为“SLProfile”的 Smart Call Home 配置文件，该文件用于指定许可颁发机构的 URL。

配置定期智能软件许可

要与思科许可证颁发机构通信，您可以选择配置 HTTP 代理。要向许可证颁发机构注册，必须在 Firepower 4100/9300 机箱上输入您从智能软件许可证账户获得的注册令牌 ID。

过程

步骤 1 （可选）配置 HTTP 代理，第 16 页。

步骤 2 （可选）删除 Call Home URL，第 17 页

步骤 3 向许可证颁发机构注册 Firepower 安全设备，第 17 页。

（可选）配置 HTTP 代理

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。

注释 不支持认证的HTTP代理。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。

Call Home 页面提供用于配置许可证颁发机构的目的地址 URL 以及配置 HTTP 代理的字段。

注释 除非获得思科 TAC 的指示，否则不应更改许可证颁发机构 URL。

步骤 2 在“服务器启用 (Server Enable)”下拉列表中，选择**开 (on)**。

步骤 3 在**服务器 URL (Server URL)** 和 **服务器端口 (Server Port)** 字段中输入代理 IP 地址和端口。例如，为 HTTPS 服务器输入端口 443。

步骤 4 单击**保存 (Save)**。

（可选）删除 Call Home URL

使用以下程序删除先前配置的 Call Home URL。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。

步骤 2 在 **Call home 配置 (Call home Configuration)** 区域中，选择删除 (Delete)。

向许可证颁发机构注册 Firepower 安全设备

当注册 Firepower 4100/9300 机箱 时，许可证颁发机构会为 Firepower 4100/9300 机箱 与许可证颁发机构之间的通信颁发 ID 证书。它还会将 Firepower 4100/9300 机箱 分配到相应的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 Firepower 4100/9300 机箱。

过程

步骤 1 在智能软件管理器或智能软件管理器卫星中，为要将此 Firepower 4100/9300 机箱添加到的虚拟账户请求并复制注册令牌。

有关如何使用智能软件管理器卫星请求注册令牌的详细信息，请参阅《思科智能软件管理器卫星用户指南》(https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html)。

步骤 2 在 Firepower 机箱管理器中，选择**系统 (System)** > **许可 (Licensing)** > **智能许可证 (Smart License)**。

步骤 3 在**输入产品实例注册令牌 (Enter Product Instance Registration Token)** 字段中输入注册令牌。

步骤 4 （可选）您可以取消选中 **Enable Cisco Success Network** 复选框以禁用 Cisco Success Network 功能。

有关详细信息，请参阅思科成功网络，第 5 页。

步骤 5 单击 **Register**。

Firepower 4100/9300 机箱尝试向许可证颁发机构注册。

要取消注册设备，请单击**取消注册 (Unregister)**。

取消注册 Firepower 4100/9300 机箱会从账户中删除设备。系统会删除设备上的所有许可证授权和证书。您可能希望取消注册来为新的 Firepower 4100/9300 机箱 释放许可证。或者，也可以从智能软件管理器删除设备。

更改 Cisco Success Network 注册

将 Firepower 4100/9300注册到思科智能软件管理器时，可启用思科成功网络。之后，可以使用以下程序查看或更改注册状态。

注释 思科成功网络在评估模式下无法工作。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Cisco Success Network**。

步骤 2 在 **Cisco Success Network 首选项 (Cisco Success Network Preferences)** 下，阅读思科提供的信息，然后单击**单击此处 (Click here)** 以查看将发送到思科的数据示例。

步骤 3 选择是否要**启用 Cisco Success Network**，然后单击**保存 (Save)**。

配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱

以下程序显示如何配置 Firepower 4100/9300 机箱以使用智能许可证卫星服务器。

开始之前

- 满足智能软件许可必备条件，第 15 页中列出的所有必要条件。
- 部署和设置智能软件卫星服务器：

  从 Cisco.com 下载智能许可证卫星 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安装指南》。
- 验证智能软件卫星服务器的 FQDN 是否可以被您的内部 DNS 服务器解析。
- 验证卫星信任点是否已存在：

  scope security

  show trustpoint

  请注意，FXOS 版本 2.4(1) 及更高版本中默认添加信任点。如果信任点不存在，则必须采用以下步骤手动添加一个信任点：

  1. 转至 http://www.cisco.com/security/pki/certs/clrca.cer，并将完整的 SSL 证书正文 （从“-----BEGIN CERTIFICATE-----”到“-----END CERTIFICATE-----”）复制到您在配置期间可访问的某个位置。
  2. 进入安全模式：

     scope security

3. 创建并命名信任点：

   create trustpoint *trustpoint_name*

4. 为信任点指定证书信息。注意：证书必须采用 Base64 编码 X.509 (CER) 格式。

   set certchain *certchain*

   对于 *certchain* 变量，粘贴您在步骤 1 中复制的证书文本。

   如果在命令中未指定证书信息，系统会提示您输入证书或定义根证书颁发机构 (CA) 的证书路径的一系列信任点。在您输入信息的下一行，键入 **ENDOFBUF** 以完成操作。

5. 提交配置：

   commit-buffer

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。

步骤 2 在 **Call home 配置 (Call home Configuration)** 区域中，采用在此程序必备条件中收集的信息，将**地址 (Address)** 字段中的默认 URL 替换为智能软件卫星服务器的 URL，格式如下：**https://***[FQDN of Satellite server]***/Transportgateway/services/DeviceRequestHandler**

步骤 3 向许可证颁发机构注册 Firepower 安全设备，第 17 页。请注意，必须从智能许可证管理器卫星请求和复制注册令牌。

配置永久许可证预留

您可以为 Firepower 4100/9300 机箱分配一个永久许可证。此通用预留允许您在设备上不受计数限制地使用任何授权。

注释 在开始之前，您必须购买永久许可证，才能在智能软件管理器中使用。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。

安装永久许可证

以下程序介绍如何为您的 Firepower 4100/9300 机箱分配永久许可证。

过程

步骤 1 选择**System**> **Licensing** > **Permanent License**。

步骤 2 单击**Generate**生成预留申请代码。将预留申请代码复制到剪贴板。

步骤 3 转至思科智能软件管理器门户的“智能软件管理器库存”屏幕，单击**Licenses**选项卡：

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

Licenses选项卡显示与您的账户相关的所有现有许可证（普通类型和永久类型）。

步骤 4 单击**License Reservation**，并将生成的预留申请代码粘贴到框中。

步骤 5 单击 **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。

如果您未看到**License Reservation**按钮，则您的账户无权使用永久许可证预留。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 6 在 Firepower 机箱管理器中，向**Authorization Code**文本框中输入生成的授权代码。

步骤 7 单击 **Install**。

在您的 Firepower 4100/9300 机箱完全获得 PLR 许可后，“永久许可证”页面将显示您的许可证状态，并提供返还永久许可证的选项。

步骤 8 在 ASA 逻辑设备上启用功能授权。请参阅 ASA 授权章节以启用授权。

（可选）返还永久许可证

如果不再需要永久许可证，您必须使用以下程序将其正式返还给智能软件管理器。如果不遵循所有步骤，许可证将保持使用状态，无法在其他地方使用。

过程

步骤 1 选择**System**> **Licensing** > **Permanent License**。

步骤 2 单击**Return**生成返还代码。将返还代码复制到剪贴板。

Firepower 4100/9300 机箱会立即变成未获许可并转变为“评估”状态。

步骤 3 访问“智能软件管理器库存”屏幕，单击**Product Instances**选项卡：

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

步骤 4 使用通用设备标识符 (UDI) 搜索您的 Firepower 4100/9300 机箱。

步骤 5 选择**Actions** > **Remove**，并将生成的返还代码粘贴到框中。

步骤 6 单击 **Remove Product Instance**。

永久许可证被返还到可用池。

步骤 7 重启系统。有关如何重新引导您的 Firepower 4100/9300 机箱的详细信息，请参阅重新启动 Firepower 4100/9300 机箱。

智能软件许可历史记录

功能名称	平台版本	说明
思科成功网络	2.7.1	思科成功网络是一项用户启用的云服务。启用思科成功网络时，Firepower 4100/9300 机箱与思科云之间会建立安全连接以传输使用情况信息和统计信息。流传输遥测数据可以提供一种机制，用于从 ASA 选择感兴趣的数据，并使用结构化格式将其传输到远程管理站，以便执行以下任务： • 向您告知在网络中可用来改进产品效果的未使用功能。 • 向您告知可能适用于您的产品的其他技术支持服务和监控。 • 帮助思科改善我们的产品 当您注册 Cisco Success Network 后，机箱总是会建立并维护安全的连接。您可以通过禁用思科成功网络随时关闭此连接，这样会将设备与思科成功网络云断开。 引入了以下命令： **scope telemetry {enable | disable}** 引入了以下菜单项： **系统 > 许可 > Cisco Success Network**

功能名称	平台版本	说明
面向 Firepower 4100/9300 机箱的思科智能软件许可	1.1(1)	通过智能软件许可，您可以购买和管理许可证池。智能许可证不与特定序列号关联。您可以轻松部署或停用设备，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。智能软件许可配置划分为 Firepower 4100/9300 机箱管理引擎和安全模块两部分。 引入了以下屏幕： **系统** > **许可** > **Call Home** **系统** > **许可** > **智能许可证**