配置安全Web设备的初始设置

目录

简介

本文档介绍首次配置安全网络设备(SWA)所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA管理。
- 基本网络原则。

Cisco 建议您：

- 已安装物理或虚拟SWA。
- 对SWA图形用户界面(GUI)的管理权限。
- 对SWA命令行界面(CLI)的管理访问。
- 对SWA控制台的管理访问。
- 有效的SWA许可证或智能许可证管理门户访问权限（如果使用智能许可证）。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

安装SWA

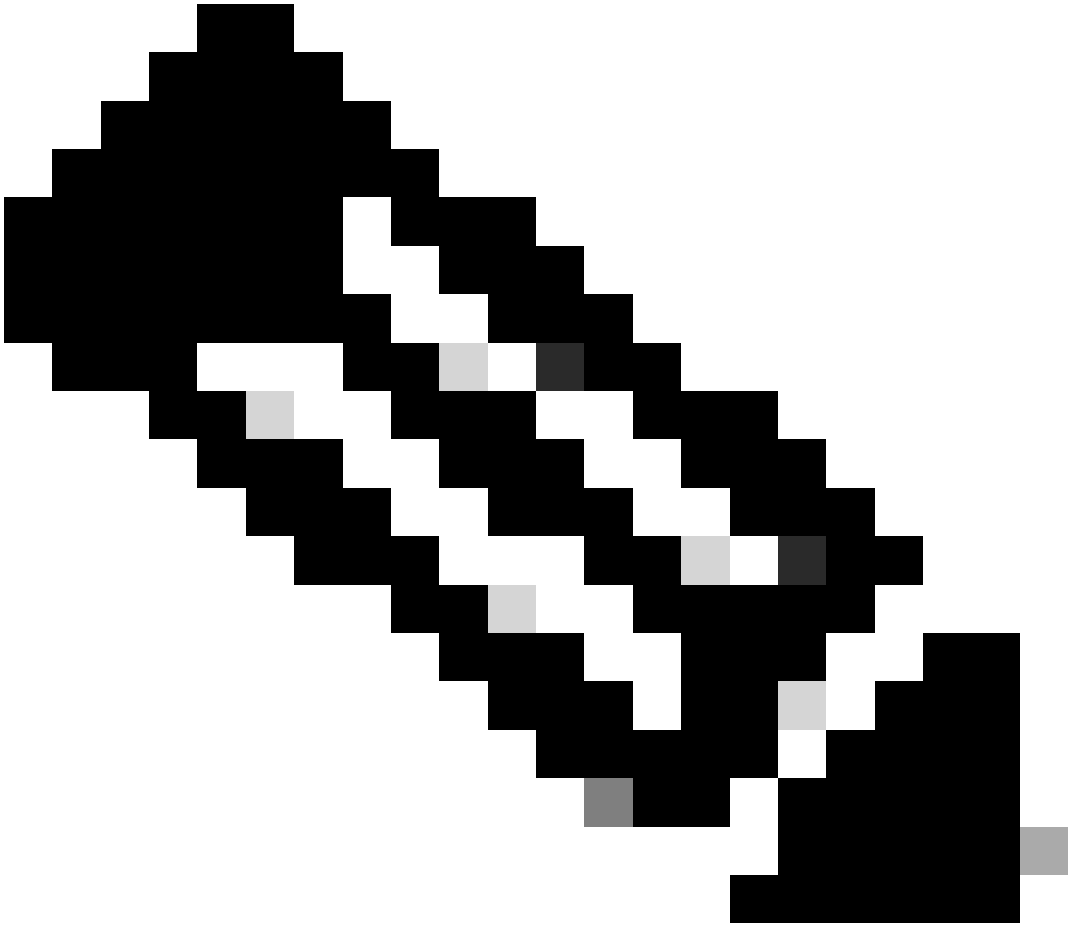
Cisco SWA是一种转发代理解决方案，旨在增强组织的网络安全和控制。SWA提供虚拟和物理两种形式，提供灵活的部署选项，以满足不同的需求。虚拟SWA支持多个虚拟机监控程序平台，包括Microsoft Hyper-V、VMware ESX和KVM，确保与一系列虚拟环境的兼容性。对于喜欢物理设备的客户，思科提供三种不同的型号：S100、S300和S600。每种模式都旨在满足不同级别的性能和容量要求，确保组织能够找到适合其特定Web安全需求的解决方案。

要下载虚拟机镜像，您可以访问：https://software.cisco.com/download/home。

安装虚拟Cisco SWA是一个直截了当的过程，从选择适当的虚拟机监控程序平台开始。首先，从思科网站下载虚拟SWA安装文件。对于VMware ESX，请部署OVA文件，确保您配置网络设置并分配足够的资源，如CPU、内存和存储。对于Microsoft Hyper-V，请将下载的VHD文件导入Hyper-V管理器，并相应地配置虚拟机设置。对于KVM，请使用virt-manager或virsh命令行工具定义和启动使用下载的映像的虚拟机。虚拟机启动并运行后，您可以使用本文中的步骤进行初始设置。

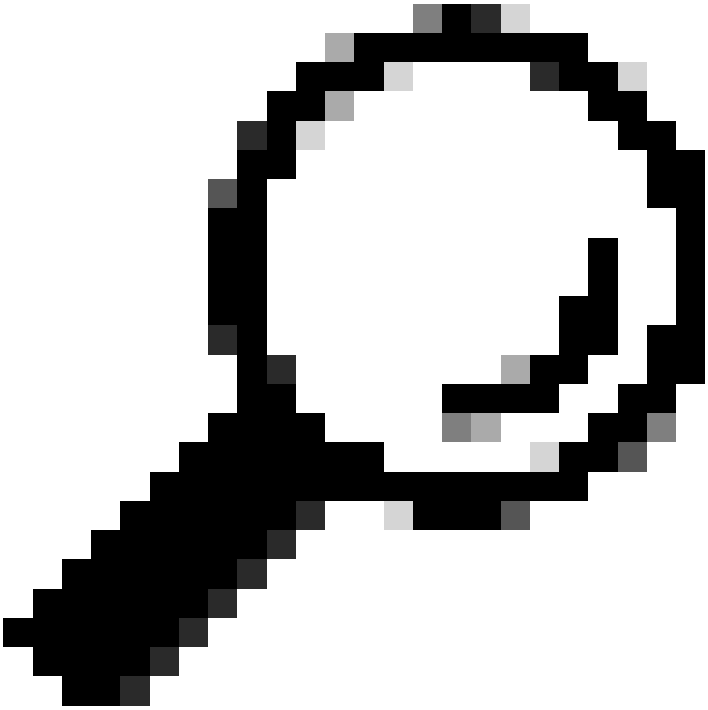
初始设置

安装SWA后，请继续执行以下步骤进行初始部署。

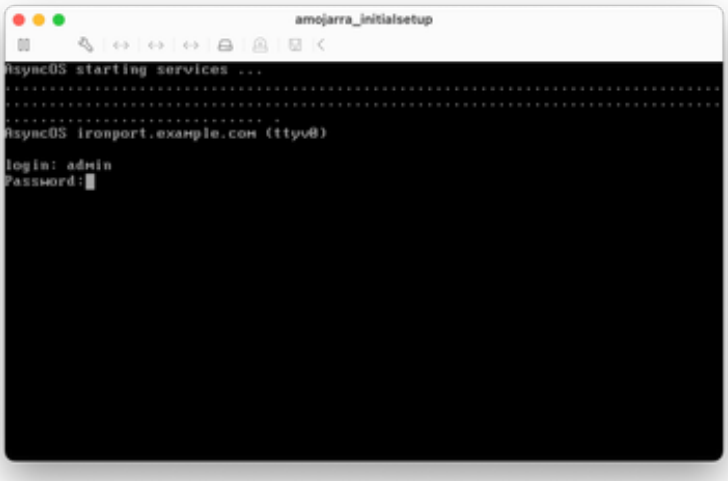


注意：对于初始设置，您需要通过控制台、SSH和GUI访问SWA。

连接方法	阶段	配置步骤
控制台	配置IP地址	步骤1:输入用户名和密码以登录CLI。



提示：默认用户名为admin，默认密码为ironport。



图像-登录屏幕

第二步：运行ifconfig。

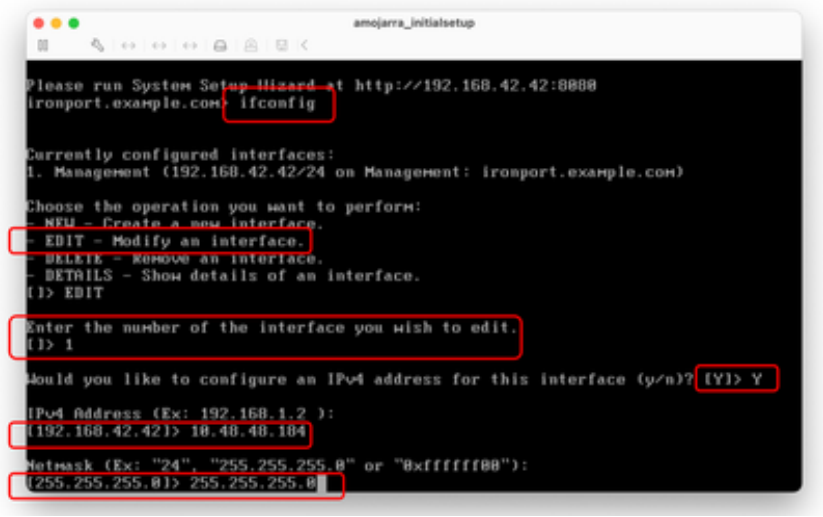
第三步：选择 Edit。

第四步：输入与管理接口关联的号码。

第五步：选择Y以编辑默认IPv4地址。

第六步：输入IP地址

步骤 7.输入子网掩码。



映像-编辑管理接口IP地址

步骤 8如果要配置IPv6，请键入Y以回答问题“Would you like to Configure IPv6？”，否则您可以将此值保留为默认值(No)并按Enter。

步骤 9输入完全限定域名(FQDN)作为主机名。

步骤 10如果要对管理接口启用文件传输协议(FTP)访问，请选择Y，否则按Enter。

步骤 11默认情况下，安全外壳(SSH)设置为启用。建议启用SSH。键入Y继续。

第12步（可选）您可以将默认SSH端口从TCP 22更改为所需的任何端口号，只要没有其它端口冲突，按Enter键即可使用默认端口(TCP/22)。

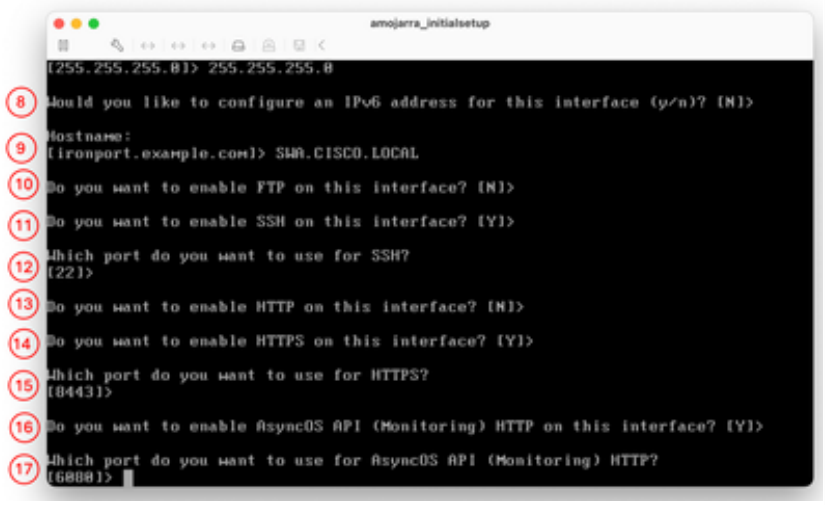
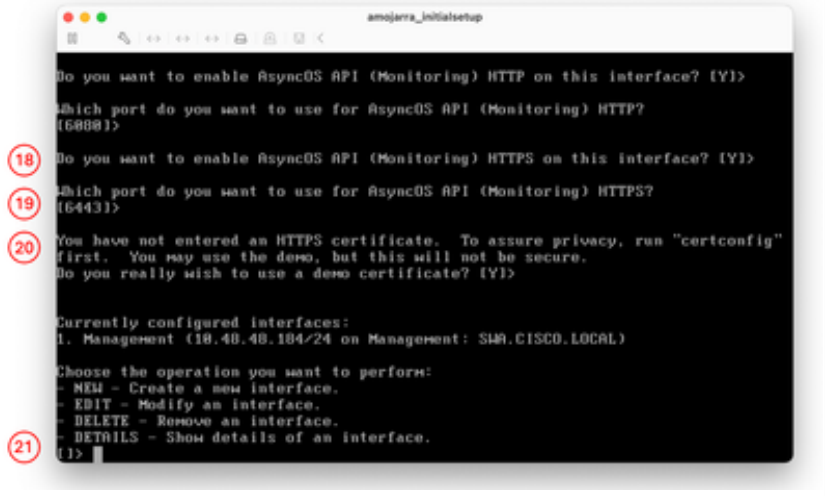
步骤 13如果要允许通过Hypertext Transfer Protocol (HTTP)访问管理接口，请键入Y并设置用于HTTP访问的端口号。否则，您可以选择N以仅对管理接口进行超文本传输协议安全(HTTPS)访问。

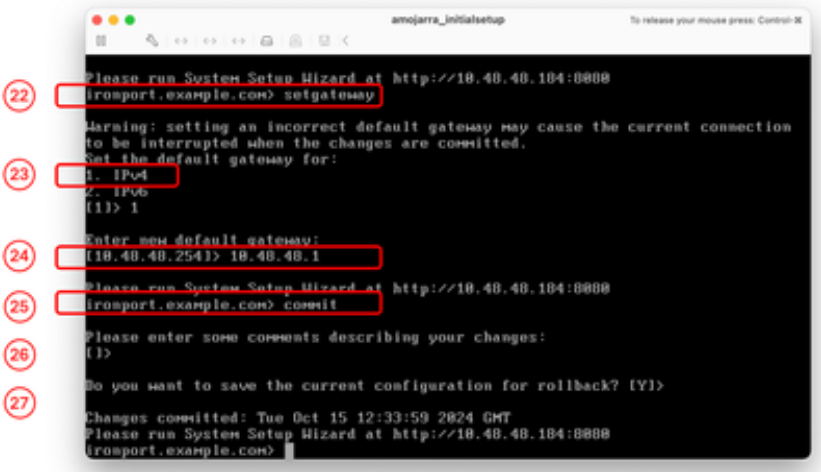
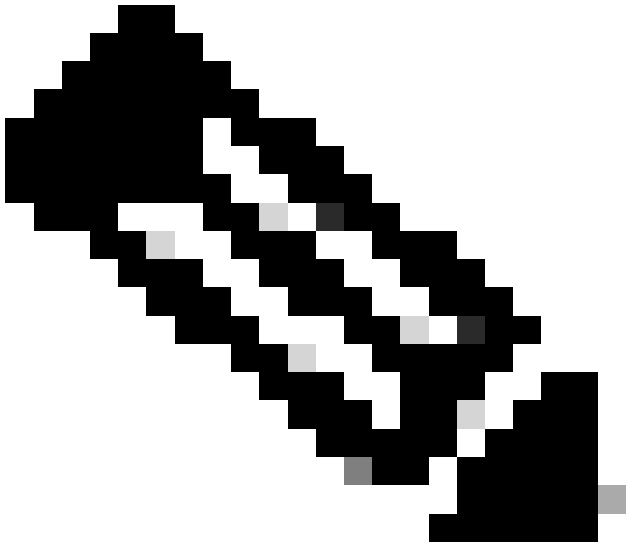
步骤 14键入Y并按Enter，以启用对管理接口的HTTPS访问。

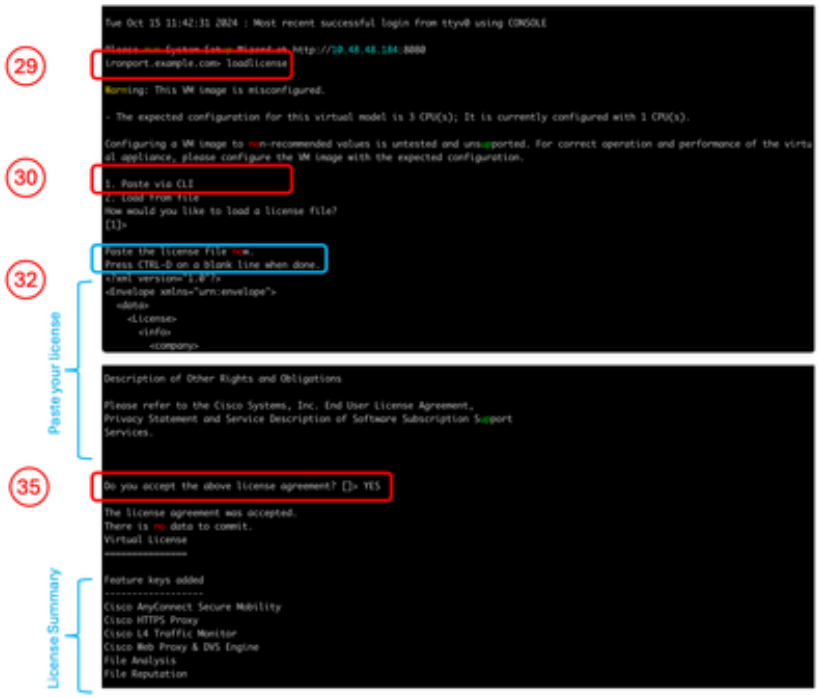
步骤 15您可以将默认HTTPS端口号从8443更改为所需的任何端口号，只要没有端口冲突，然后按Enter键使用默认端口(TCP/8443)。

步骤 16 应用程序编程接口(API)默认设置为启用，如果您不使用API，则可以通过键入N并按Enter禁用API。

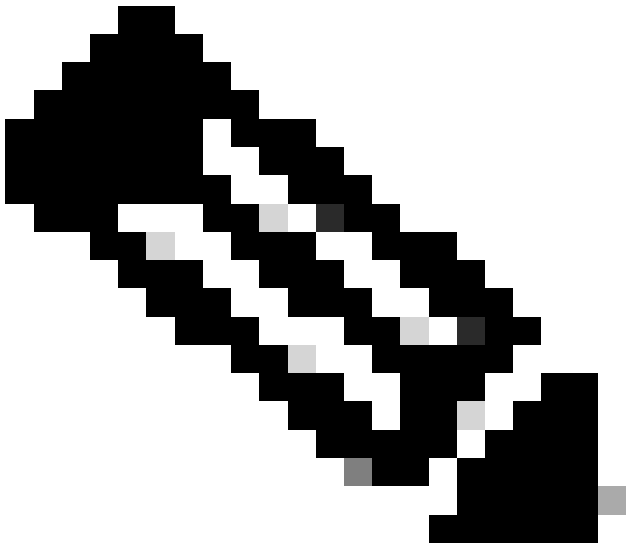
步骤 17如果您选择启用API，您可以将默认API端口号从

		6080更改为您想要的任何端口号，只要没有其他端口冲突，请按Enter使用默认端口(TCP/6080)。  映像-管理接口服务配置 步骤 18.AsyncOS API（监控）是SWA上的新GUI，如果要使用新用户界面报告，请将此选项设置为Y（默认值），否则您可以键入N并跳至第20步 步骤 19. 您可以将默认新的GUI HTTPS端口号从6443更改为所需的任何端口号，只要不存在其他端口冲突，按Enter键即可使用默认端口(TCP/6443)。 步骤 20.SWA管理接口使用思科演示证书。键入Y接受演示证书。您可以在初始设置后更改GUI证书。 步骤 21.按Enter退出ifconfig向导。  映像-新GUI TCP配置
	配置默认网关	步骤 22.运行setgateway。

		步骤 23.如果管理接口配置了IPv4，请选择IPv4，否则请选择IPv6。 步骤 24输入您的默认网关IP地址。 步骤 25通过运行commit保存更改。 第26步（可选）您可以添加有关正在保存的更改的注释 第27步（可选）您可以在应用更改之前使用SWA来备份配置。  映像-配置默认网关
SSH	导入传统许可证	 注意：如果您使用的是智能许可证，请跳到第36步。

		步骤 28 通过SSH连接到SWA。 步骤 29运行loadlicense 步骤 30选择通过CLI粘贴。 步骤 31 使用文本编辑器打开许可证文件，并复制其所有内容 步骤 32将许可证粘贴到SSH外壳中。 步骤 33按Enter导航到新行。 步骤 34按住Control并按D。 步骤 35阅读许可协议并键入YES同意条件。  映像-导入传统许可证 跳至步骤58。
GUI	配置DNS服务器	步骤 37 登录GUI(默认值为HTTPS://<SWA FQDN或IP地址>：8443) 步骤 38导航到网络并选择DNS。 步骤 39单击 Edit Settings。 第40步：在主DNS服务器部分中，选择使用这些DNS服务器。

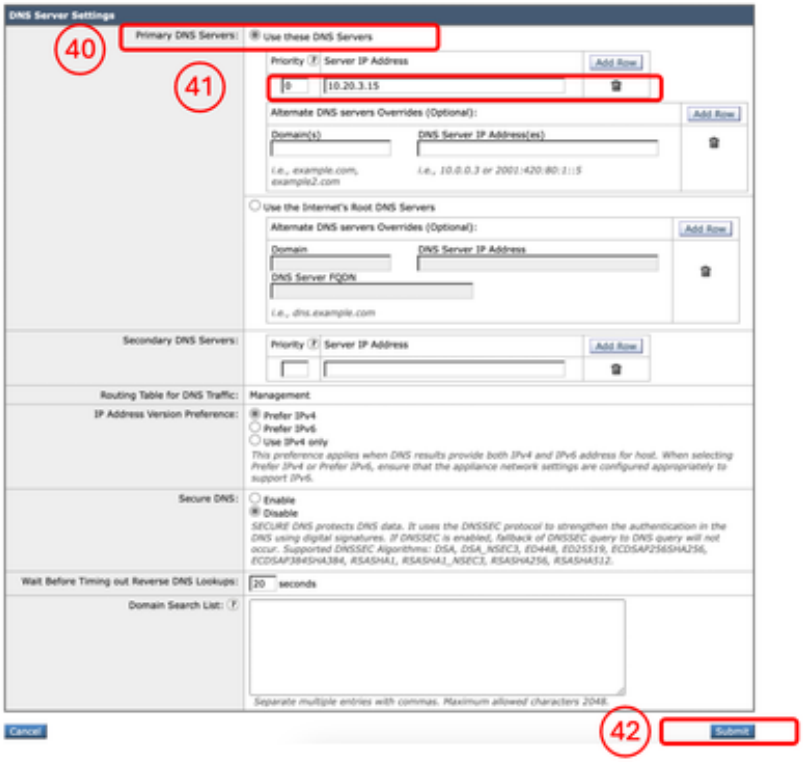
步骤 41将优先级设置为0并输入您的DNS服务器IP地址。



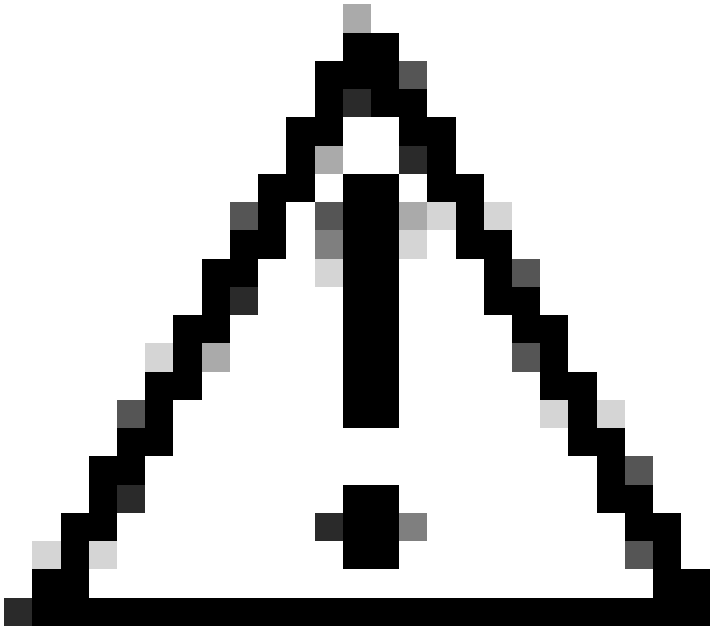
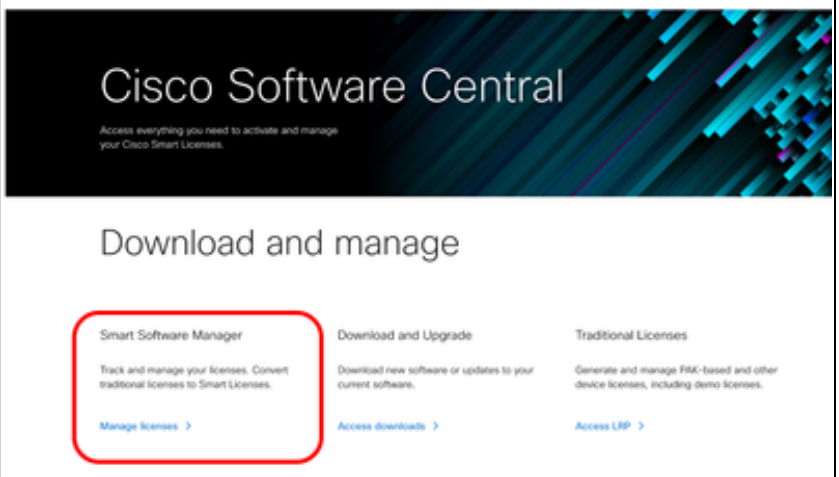
注意：您可以通过选择添加行来添加多个DNS服务器。

步骤 42提交。

步骤 43提交更改。



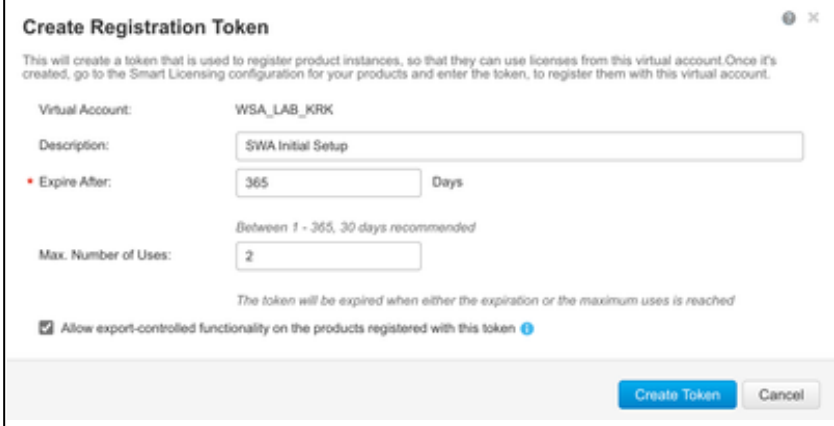
映像-配置DNS服务器

	配置智能许可证	步骤 44在系统管理的GUI中，选择智能软件许可。 步骤 45 选择启用智能软件许可。  注意：在设备上启用智能许可证功能后，无法从智能许可证回滚到经典许可证。 步骤 46 点击确定以继续配置智能许可证。 步骤 47提交更改。 步骤 48 要获取用于注册SWA的令牌，请登录思科软件中心 (https://software.cisco.com/#) 步骤 49单击Manage Licenses。  图像-思科智能许可证管理 步骤 50在智能软件许可中选择资产。

步骤 51在常规选项卡中，创建新令牌或使用可用令牌。

映像-智能软件许可证资产页面

步骤 52输入所需信息和创建令牌。

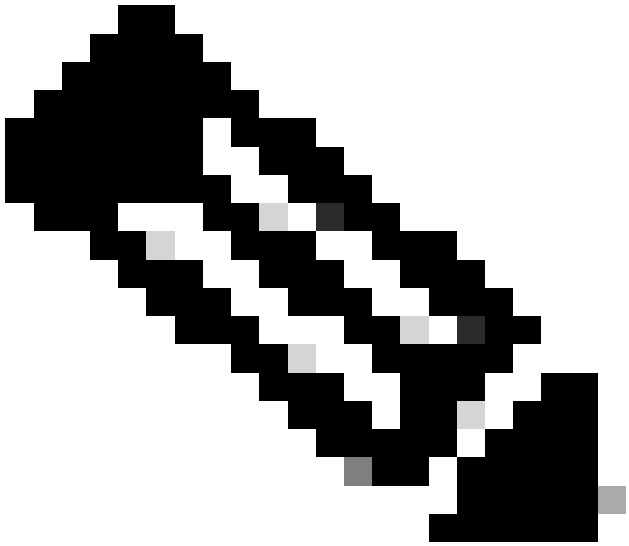
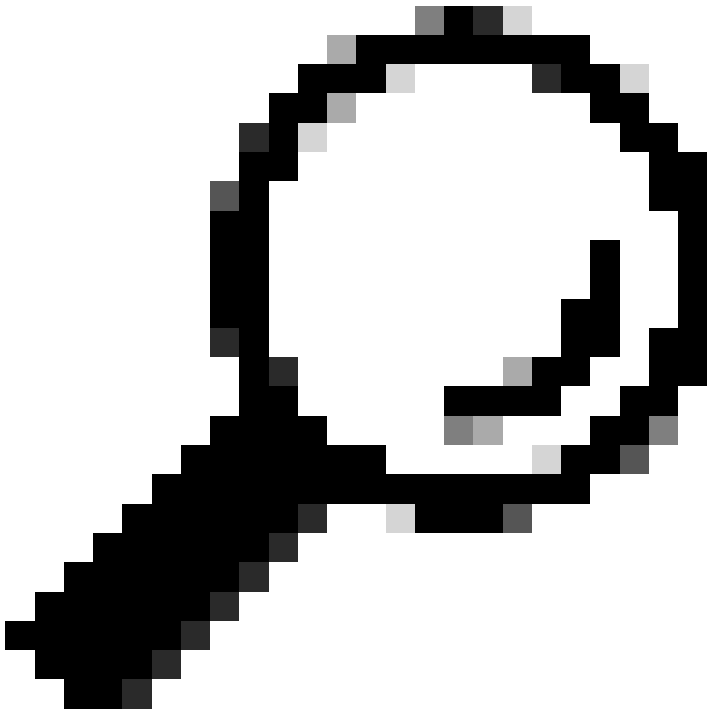


图像-生成令牌

步骤 53单击新添加的令牌前面的蓝色图标并复制其内容。

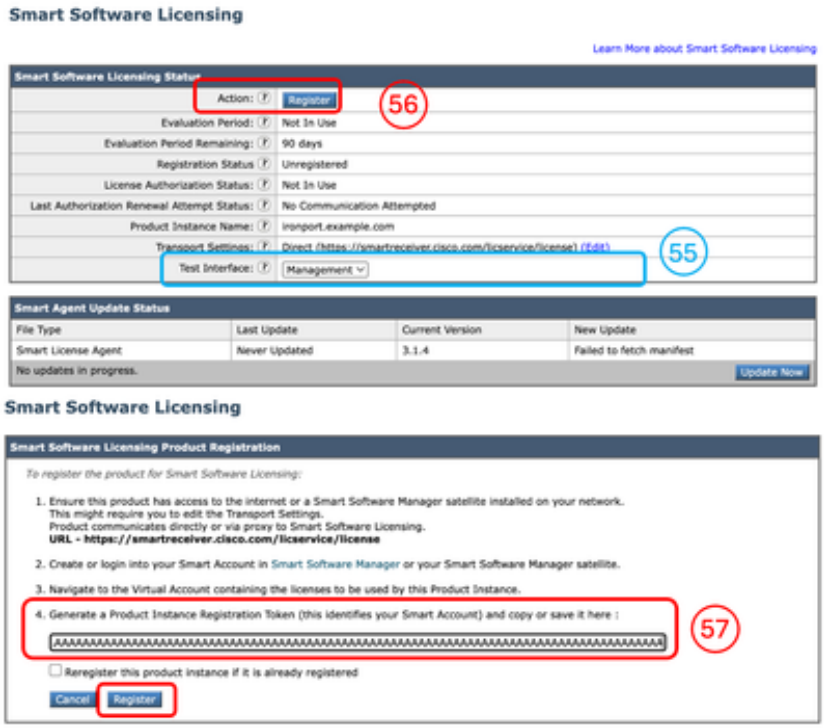
映像-复制令牌

步骤 54 在SWA GUI中，导航至系统管理并选择智能软件许可。

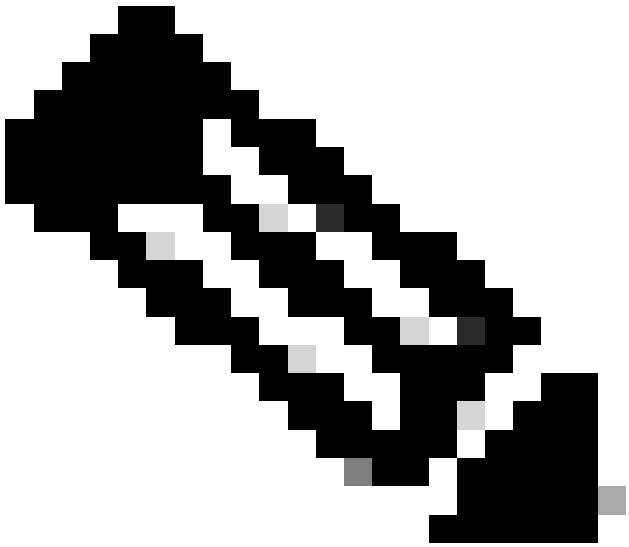
		 注意：如果您已经位于智能软件许可页面，请刷新该页面。 第55步（可选）如果SWA不能从管理接口访问互联网，您可以将测试接口更改为允许访问互联网的接口。  提示：有关多个接口配置和路由表的详细信息，请检查本文的“网络配置”部分。

步骤 56点击注册。

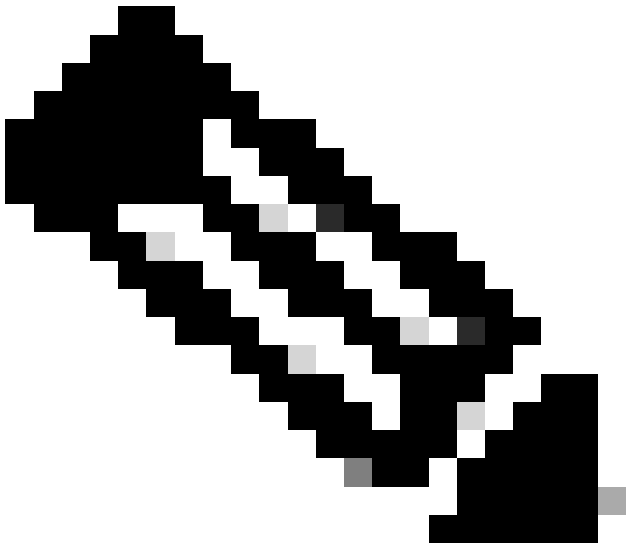
步骤 57粘贴令牌并单击注册。

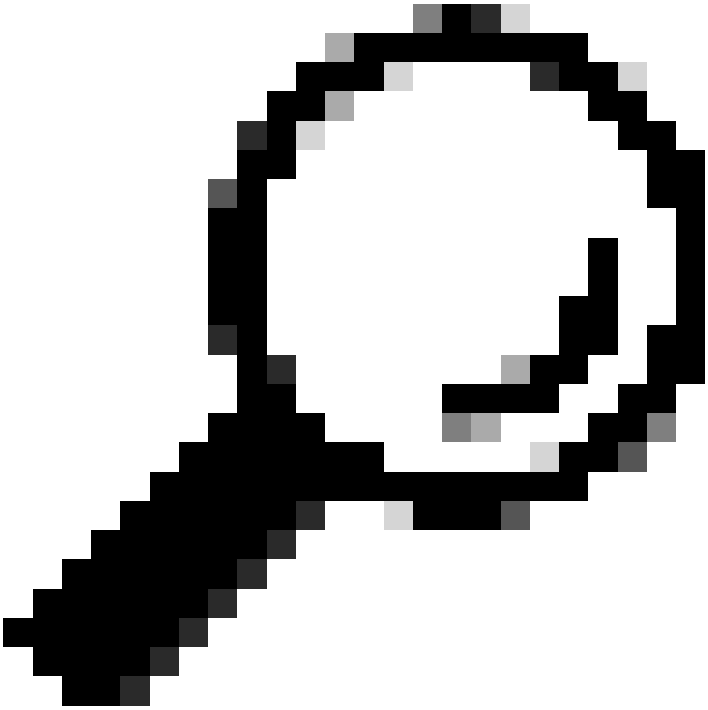


图像-将SWA注册到智能许可证



注意：要验证您的注册，请等待几分钟，刷新SWA中的智能许可页面，并检查注册状态。

		 图像-智能许可证注册状态
	系统设置向导	步骤 58 在SWA GUI中，导航到系统管理并选择系统设置向导。 步骤 59阅读并接受本许可协议的条款 步骤 60单击Begin Setup。 步骤 61选择 标准来自 装置操作模式部分。 步骤 62输入Default System Hostname。  注意：第9步中创建的以前主机名与管理接口相关，与SWA无关。 步骤 63输入DNS服务器IP地址。 第64步：您可以配置网络时间协议(NTP)服务器。

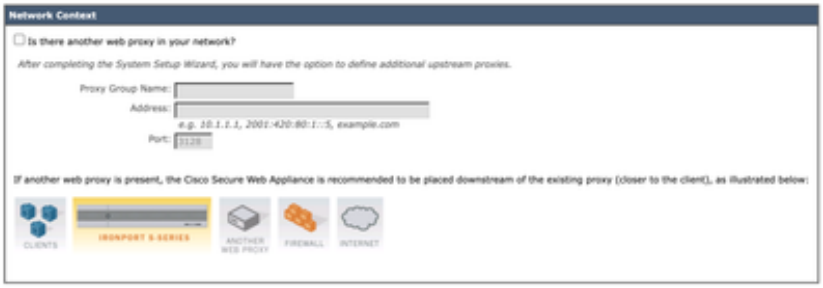


提示：如果您的NTP服务器需要身份验证，您可以配置密钥参数。

步骤 65选择应用于SWA的时区，然后单击下一步。

映像-系统设置向导-系统设置

第66步（可选）如果您正在使用网络中的任何上游代理，则可以在Network Context页面上配置它，或者保留其为默认值并点击下一步(Next)。

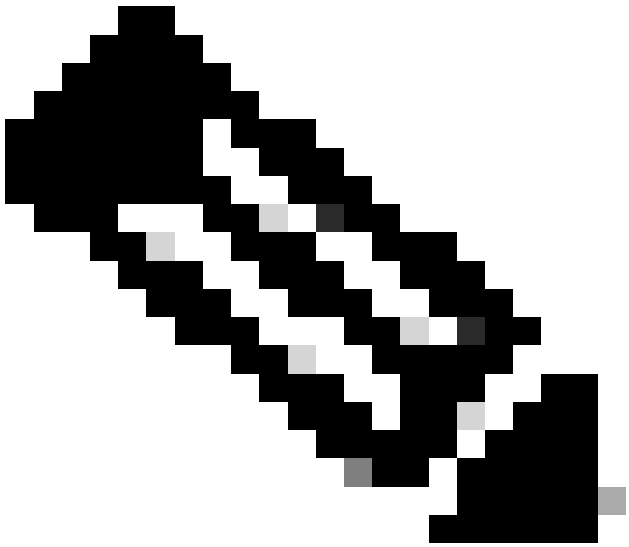


映像-系统设置向导-上游代理配置

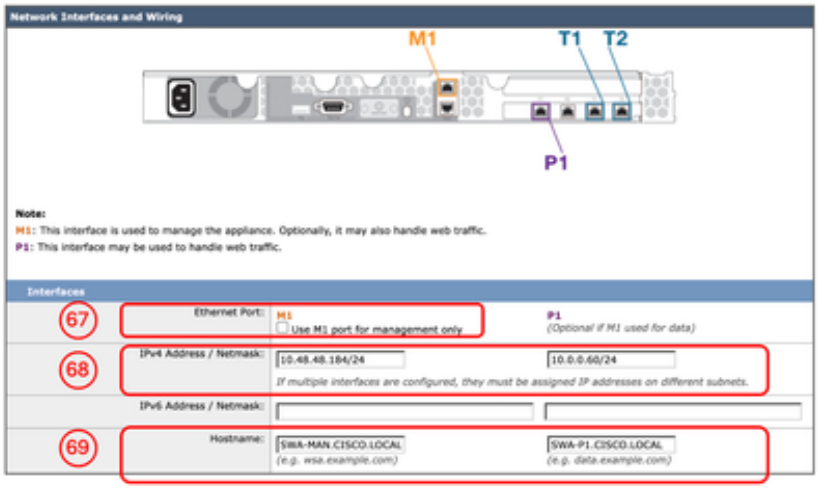
第67步（可选）如果需要将管理接口流量与数据接口（P1和P2接口）流量分开，请选择Use M1 port for management only。

第68步（可选）您可以从IPv4地址/网络掩码或IPv6地址/网络掩码部分添加或修改网络接口IP地址。

第69步（可选）您可以添加或修改网络接口主机名并点击下一步(Next)。

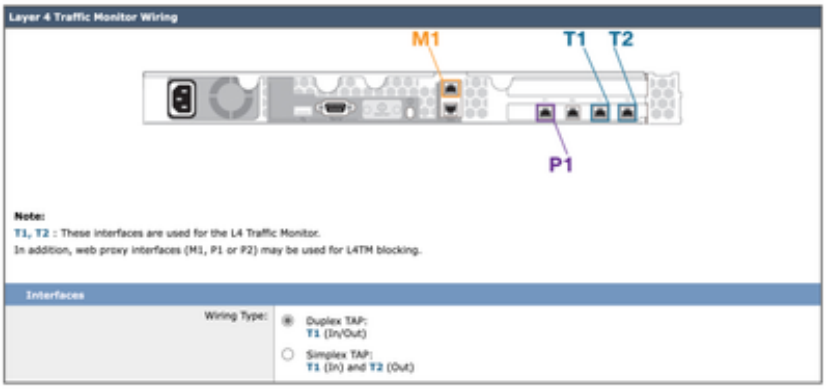


注意：可以通过系统设置向导启用和配置P1端口。如果要启用P2接口，必须在完成“系统设置向导”(System Setup Wizard)后完成此操作。



映像-系统设置向导-网络接口配置

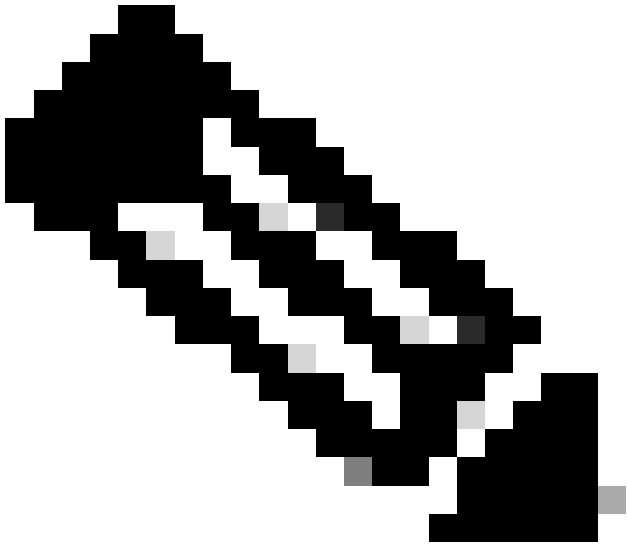
第70步（可选）如果计划配置第4层流量监控器(L4TM)，可以配置双工设置，也可以保留默认设置，然后点击下一步(Next)。



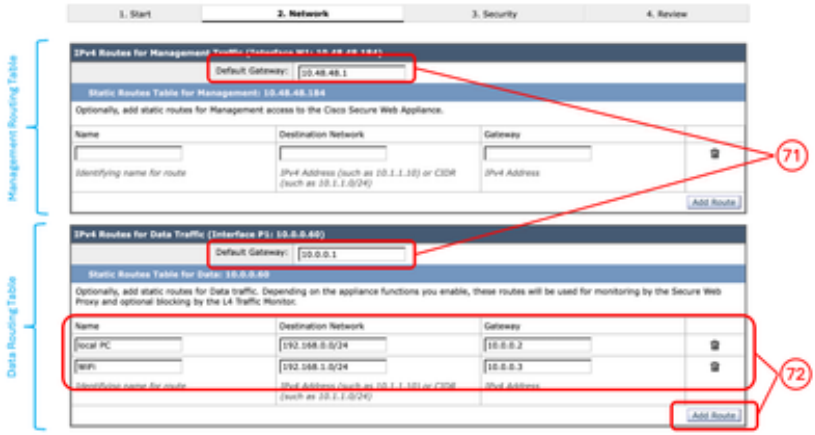
映像-系统设置向导-第4层流量监控器设置

第71步（可选）在IPv4 Routes for Management页面中，您可以修改默认网关

步骤72.（可选）您可以添加路由来创建静态路由。

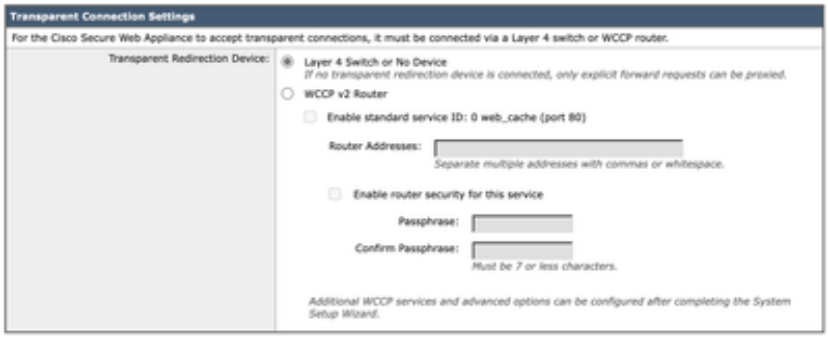


注意：如果在第67步中选择“Use M1 port for management only”，则管理接口和数据接口（P1和P2）将有两个单独的路由表。



映像-系统设置向导-添加路由

第73步（可选）如果要通过Web缓存通信协议(WCCP)设置透明代理部署，可以配置WCCP设置，或者可以保留默认的第4层交换机或无设备，然后点击下一步。



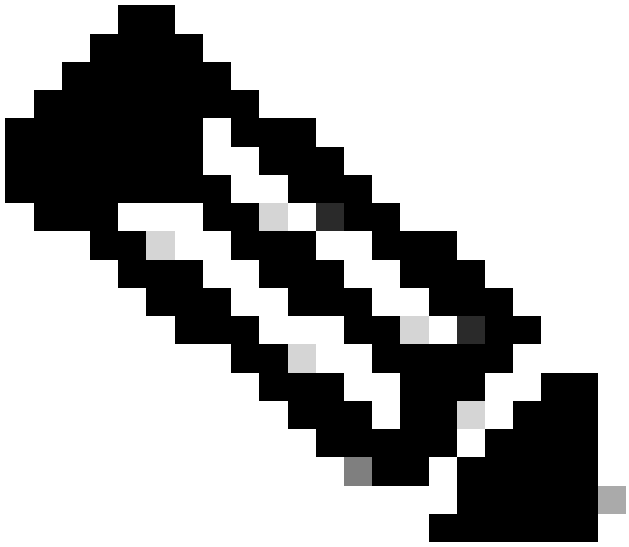
映像-系统设置向导-代理部署配置

步骤 74为管理员帐户设置新的密码。

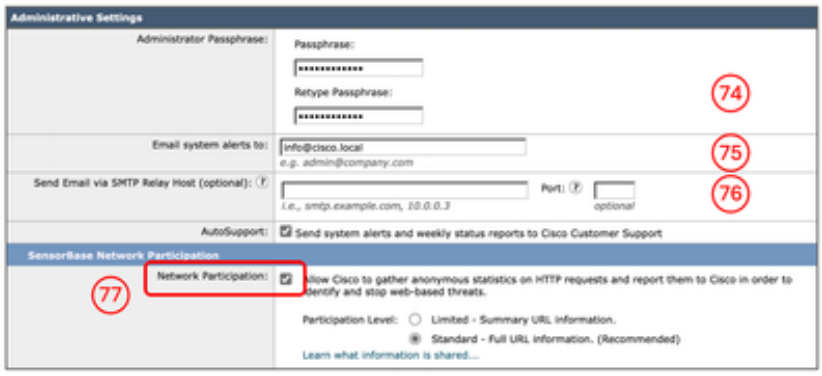
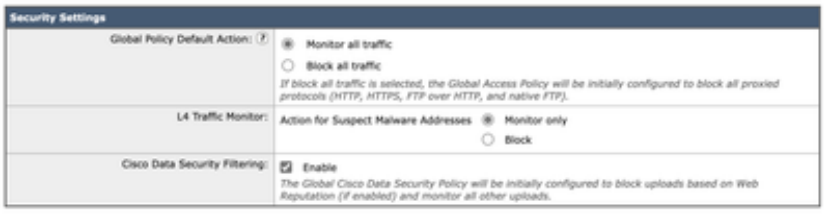
步骤 75输入预计接收系统警报的电子邮件地址。

第76步（可选）提供简单邮件传输协议(SMTP)中继主机信息，否则将其留空 如果未定义内部中继主机，SMTP将使用MX记录的DNS查找。

第77步（可选）如果要禁用参与Cisco SensorBase网络，请取消选中网络参与复选框，否则保留为默认值并点击下一步。



注意：参与Cisco SensorBase网络意味着思科收集数据并与SensorBase威胁管理数据库共享该信息。

		 映像-系统设置向导-管理设置 第78步（可选）您可以更改全局策略、L4TM和思科数据安全过滤的默认操作，也可以将其保留为默认值并单击下一步。  映像-系统设置向导-安全设置 步骤 79检查您的配置。如果需要更改，请单击Previous按钮以返回上一页，否则单击Install This Configuration。

网络配置

要配置网络接口，您可以使用CLI或GUI。

	命令/路径	操作
从CLI配置网络接口卡	CLI > ifconfig	新建：如果接口未列在ifconfig输出中，但存在于虚拟机或物理设备中，则您可以使用此命令在列表中显示接口。 Edit：此操作是编辑IP地址、子网掩码、接口主机名或其他相关参数。 详细信息：显示接口的详细信息，如MAC地址、媒体类型、双工模式等。

		Delete：从ifconfig列表中删除接口，并删除IP地址（如果之前已分配）。
从GUI配置网络接口卡	GUI > Network > Interfaces	您可以编辑接口IP地址和主机名。 您可以启用、禁用或修改 设备管理服务，如FTP、SSH、HTTP访问和HTTPS访问。

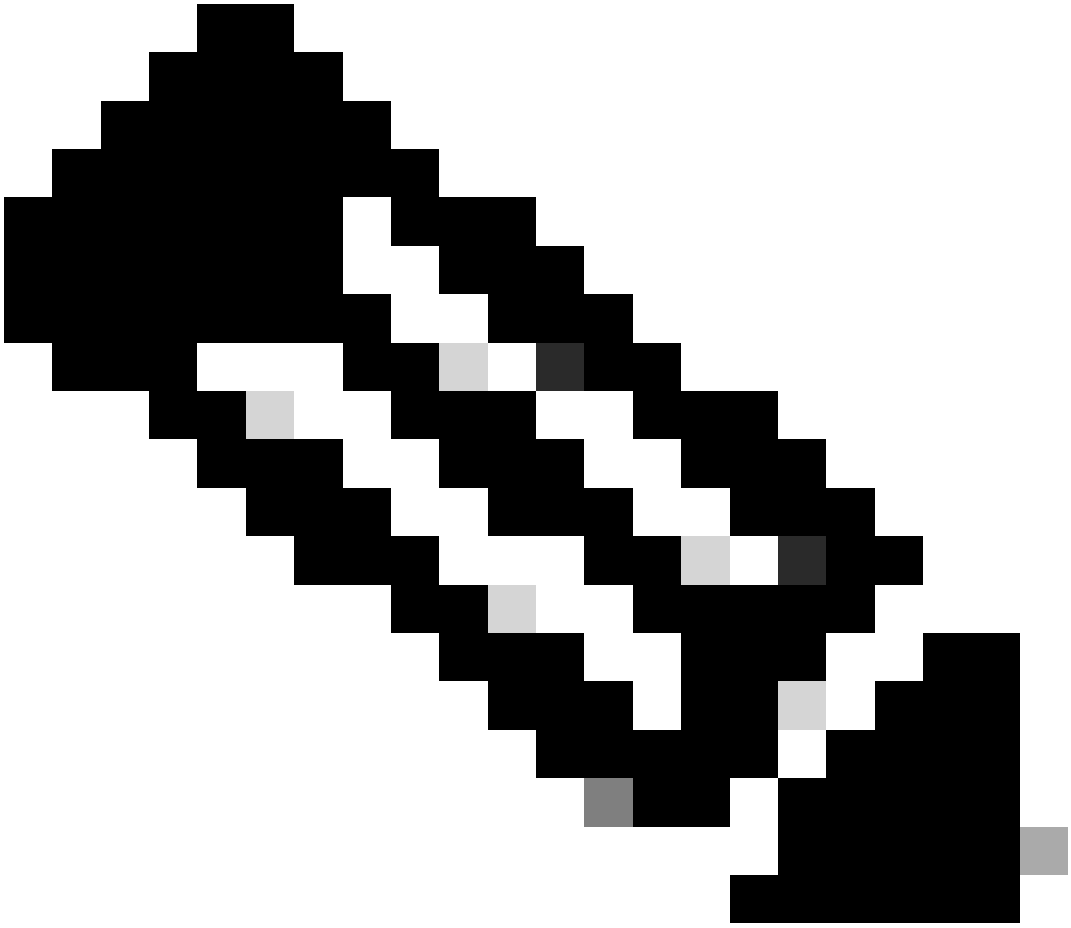
路由表

路由是确定将网络流量定向到何处必不可少的因素。SWA处理以下类型的流量：

- 数据流量：这包括网络代理从浏览互联网的最终用户处处理的流量。
- 管理流量：包括通过网络界面管理设备生成的流量，以及用于SWA升级、组件更新、DNS、身份验证和其他相关任务等管理服务的流量。

默认情况下，两种流量均使用为所有配置的网络接口定义的路由。但是，您可以选择分隔路由，以便管理流量使用专用管理路由表，而数据流量使用单独的数据路由表。

管理流量	数据流量
WebUI SSH SNMP 身份验证，带域控制器(可配置) 系统日志 FTP推送 DNS(可配置) 更新/升级/功能密钥(可配置)	HTTP 代理 HTTPS代理 FTP代理 WCCP协商 使用外部DLP服务器的ICAP请求 DNS(可配置) 更新/升级/功能密钥(可配置) 使用域控制器进行身份验证(可配置)



注意：如果选择“仅将M1端口用于管理”选项，则会向SWA添加一个称为数据路由表的附加路由表。此路由表只有一个可配置的默认网关；任何其他路由路径都必须手动配置。

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南
- 思科安全邮件和Web虚拟设备安装指南
- 在安全网络设备中配置自定义URL类别-思科
- 使用安全Web设备最佳实践
- 为安全Web设备配置防火墙
- 在安全Web设备中配置解密证书
- 在SWA中配置SNMP并对其进行故障排除

- 在带有Microsoft Server的安全Web设备中配置SCP推送日志
- 在SWA中启用特定YouTube频道/视频，并阻止YouTube的其余部分
- 了解安全Web设备中的HTTPS访问日志格式
- 访问安全Web设备日志
- 绕过安全网络设备中的身份验证
- 阻止安全Web设备中的流量
- 绕过安全Web设备中的Microsoft更新流量

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。