Configuración de la configuración inicial del dispositivo web seguro

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Instalación de SWA

Configuración inicial

- Configurar dirección IP
- Configurar puerta de enlace predeterminada
- Importar licencia tradicional
- Configurar servidor DNS
- Configurar Smart License
- Asistente de configuración del sistema

Configuración de red

Tabla de ruteo

Información Relacionada

Introducción

Este documento describe los pasos necesarios para configurar el dispositivo web seguro (SWA) por primera vez.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.
- Principios fundamentales de las redes.

Cisco recomienda que tenga:

- SWA físico o virtual instalado.
- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA.
- Acceso administrativo a la interfaz de línea de comandos (CLI) SWA.
- Acceso administrativo a la consola SWA.
- Licencia SWA válida o acceso al portal de Smart License Management (en caso de que

utilice Smart License).

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Instalación de SWA

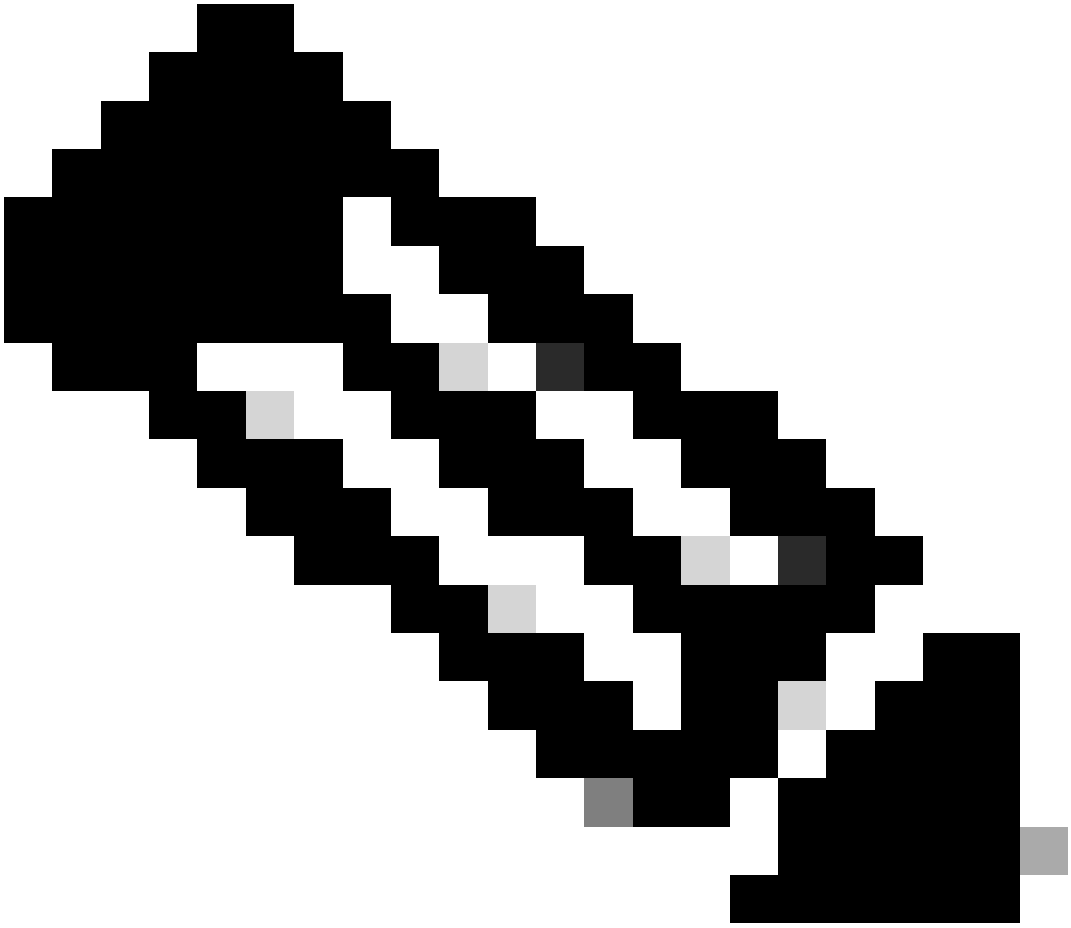
Cisco SWA es una solución de proxy directo diseñada para mejorar la seguridad web y el control de las organizaciones. Disponible en formas virtuales y físicas, el SWA proporciona opciones de implementación flexibles para satisfacer las distintas necesidades. El SWA virtual es compatible con varias plataformas de hipervisor, incluidas Microsoft Hyper-V, VMware ESX y KVM, lo que garantiza la compatibilidad con una amplia gama de entornos virtuales. Para aquellos que prefieren un dispositivo físico, Cisco ofrece tres modelos distintos: S100, S300 y S600. Cada modelo está diseñado para satisfacer diferentes niveles de rendimiento y requisitos de capacidad, lo que garantiza que las organizaciones puedan encontrar la solución adecuada para sus necesidades específicas de seguridad web.

Para descargar la imagen de la máquina virtual, visite: https://software.cisco.com/download/home .

La instalación del software Cisco ASA virtual es un proceso sencillo que comienza con la selección de la plataforma de hipervisor adecuada. En primer lugar, descargue el archivo de instalación SWA virtual desde el sitio web de Cisco. Para VMware ESX, implemente el archivo OVA, asegurándose de configurar los parámetros de red y asignar suficientes recursos como CPU, memoria y almacenamiento. Para Microsoft Hyper-V, importe el archivo VHD descargado en el Administrador de Hyper-V y configure la máquina virtual en consecuencia. Para KVM, utilice la herramienta de línea de comandos virt-manager o virsh para definir e iniciar la máquina virtual mediante la imagen descargada. Una vez que la máquina virtual está en funcionamiento, puede seguir los pasos descritos en este artículo para realizar la configuración inicial.

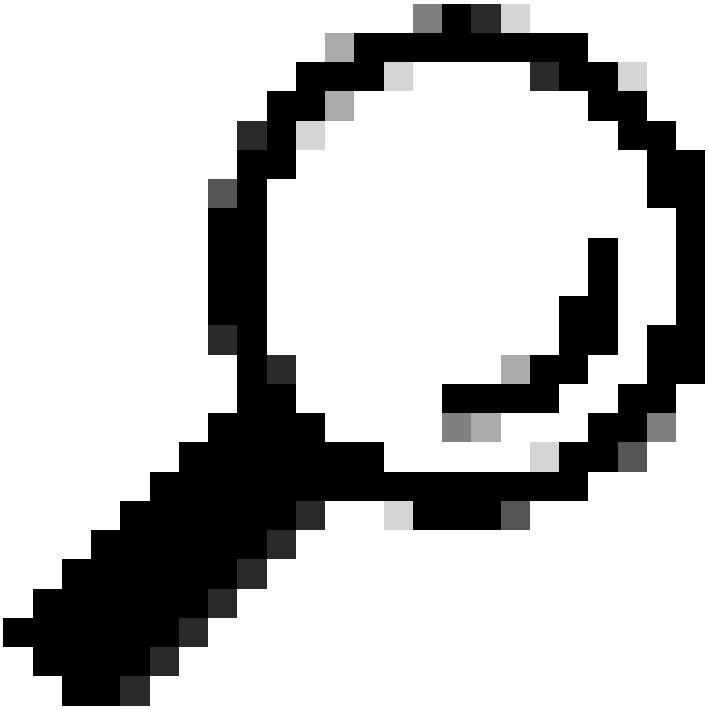
Configuración inicial

Después de instalar el SWA, continúe con estos pasos para la implementación inicial.



Nota: Para la configuración inicial, debe tener acceso a SWA a través de la consola, SSH y GUI.

Método de conexión	Fase	Configuration Steps
Consola	Configurar dirección IP	Paso 1. Introduzca el nombre de usuario y la contraseña para iniciar sesión en la CLI.



Sugerencia: el nombre de usuario predeterminado es admin y la contraseña predeterminada es ironport.

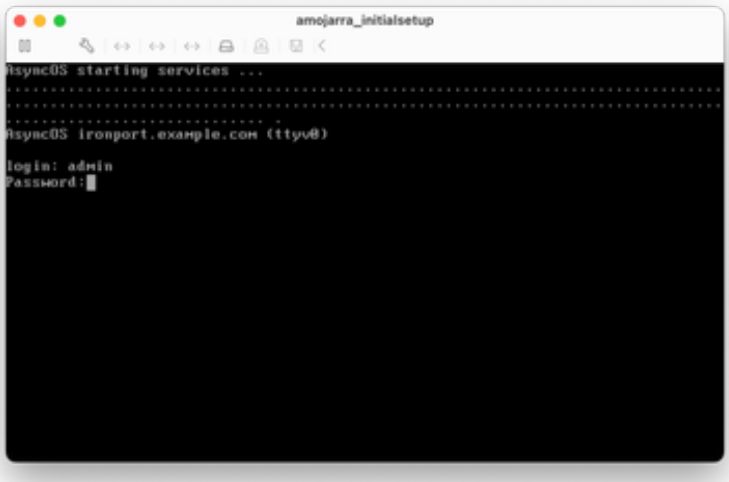


Imagen - pantalla de inicio de sesión

Paso 2. Ejecute ifconfig.

Paso 3. Elija Edit.

Paso 4. Introduzca el número asociado a la interfaz de gestión.

Paso 5. Seleccione Y para editar la dirección IPv4

predeterminada.

Paso 6. Introduzca la dirección IP

Paso 7. Introduzca la máscara de subred.

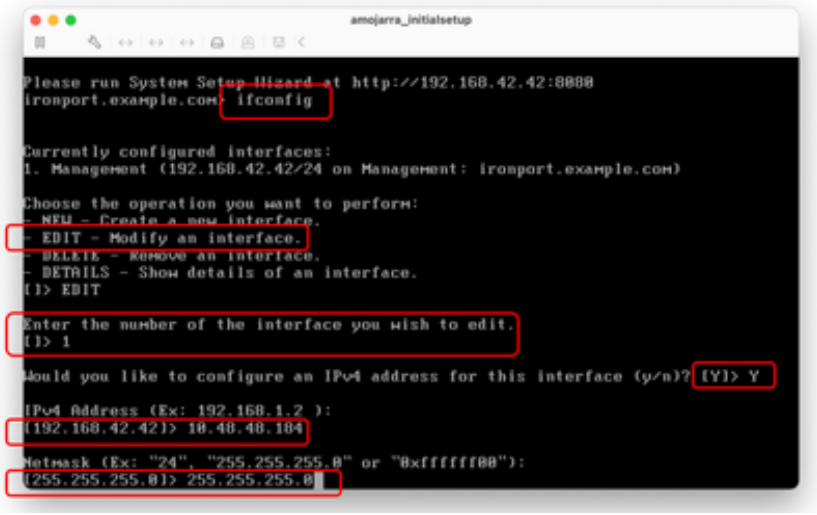


Imagen - Editar dirección IP de interfaz de administración

Paso 8. Si desea configurar IPv6, escriba Y en respuesta a la pregunta "¿Desea configurar IPv6?"; de lo contrario, puede dejar esto como predeterminado (No) y presionar Intro.

Paso 9. Introduzca un nombre de dominio completo (FQDN) como nombre de host.

Paso 10. Si desea habilitar el acceso del protocolo de transferencia de archivos (FTP) a la interfaz de administración, elija Y, o bien presione Enter.

Paso 11. El Secure Shell (SSH) se establece en Enabled (Activado) de forma predeterminada. se recomienda tener el SSH activado. Escriba Y para continuar.

Paso 12. (Opcional) Puede cambiar el puerto SSH predeterminado de TCP 22 a cualquier número de puerto que desee, siempre y cuando no haya conflictos entre puertos, presione Enter para utilizar el puerto predeterminado (TCP/22).

Paso 13. Si desea tener acceso al protocolo de transferencia de hipertexto (HTTP) a la interfaz de administración, escriba Y y establezca el número de puerto para el acceso HTTP. De lo contrario, puede elegir N para tener acceso seguro al Protocolo de transferencia

de hipertexto (HTTPS) solamente a la interfaz de administración.

Paso 14. Escriba Y y pulse Intro para activar el acceso HTTPS a la interfaz de gestión.

Paso 15. Puede cambiar el número de puerto HTTPS predeterminado de 8443 a cualquier número de puerto que desee, siempre y cuando no haya conflictos entre puertos. Pulse Intro para utilizar el puerto predeterminado (TCP/8443).

Paso 16. De forma predeterminada, la interfaz de programación de aplicaciones (API) está establecida en Habilitar. Si no está utilizando API, puede deshabilitar la API escribiendo N y presionando Intro.

Paso 17. Si elige tener la API habilitada, puede cambiar el número de puerto API predeterminado de 6080 a cualquier número de puerto que desee, siempre y cuando no haya conflictos de puertos, presione entrar para utilizar el puerto predeterminado (TCP/6080).

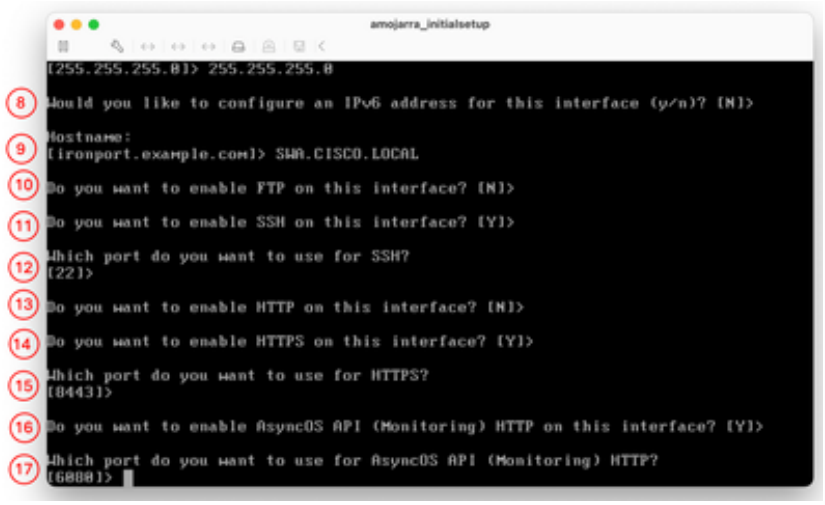
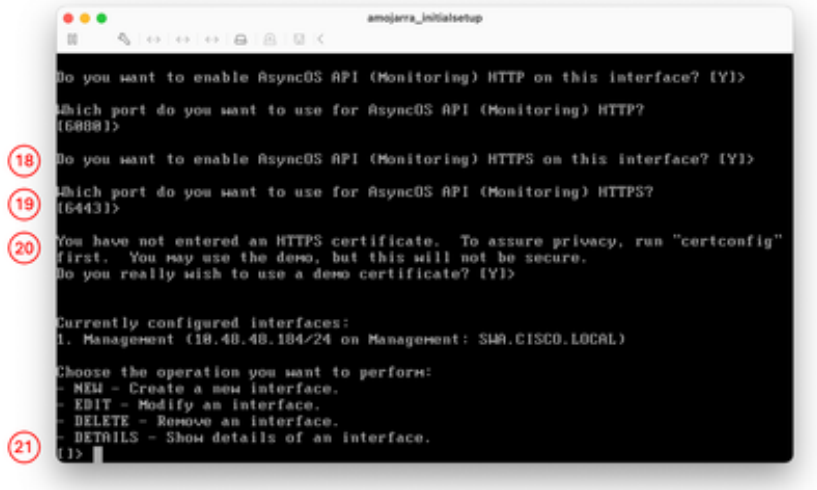
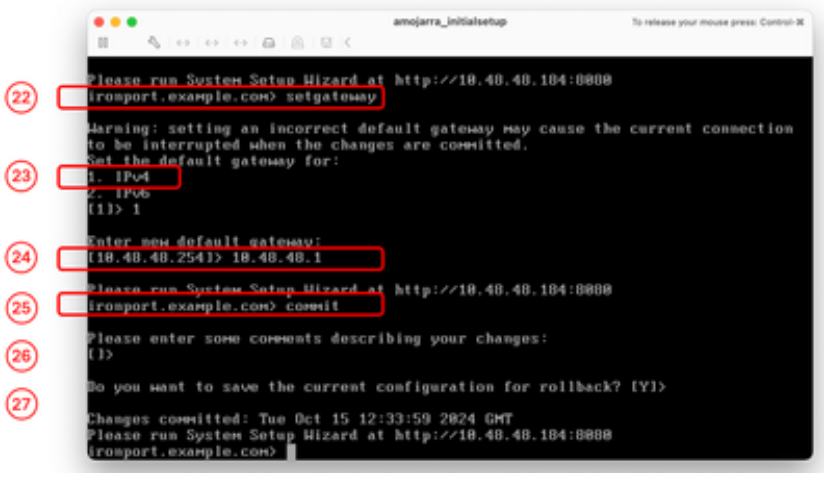
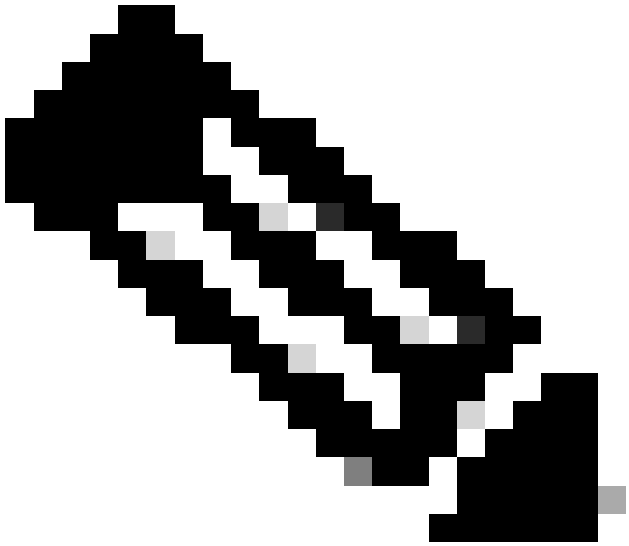


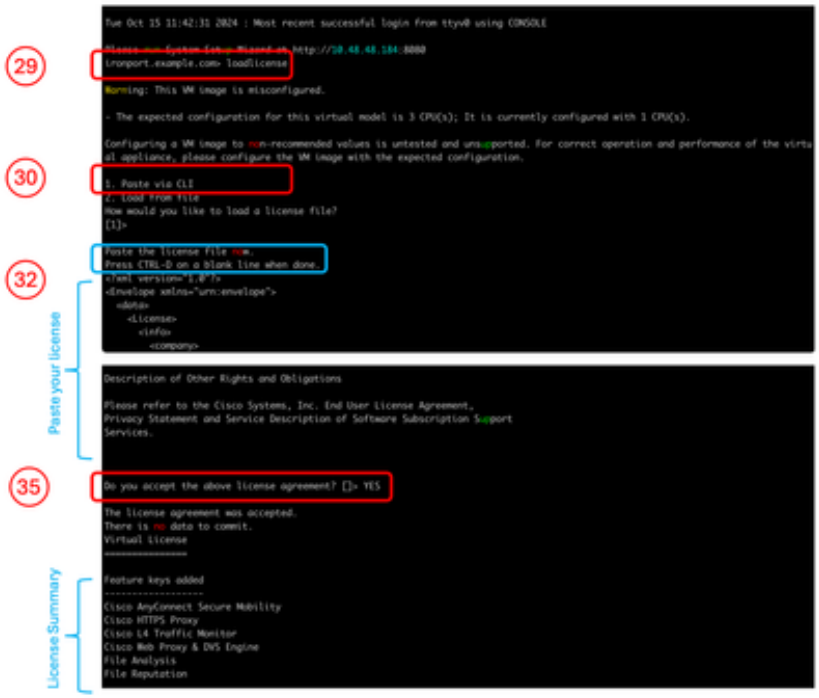
Imagen - Configuración del servicio de interfaz de administración

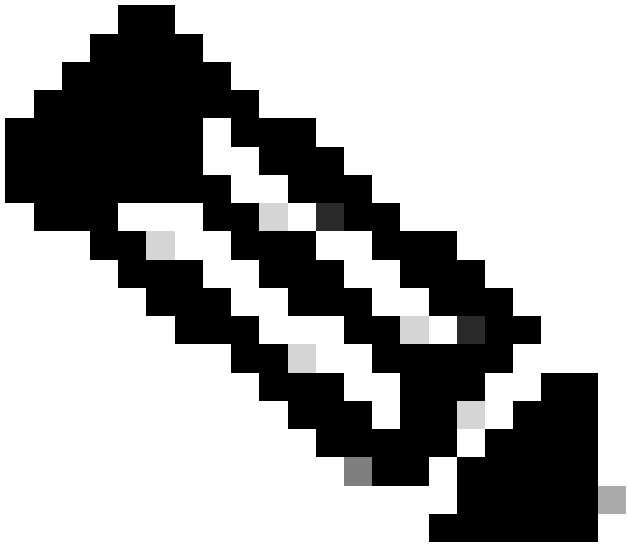
Paso 18. API AsyncOS (monitoreo) es la nueva GUI en el SWA, si desea utilizar los nuevos informes de la interfaz de usuario, establezca esta opción en Y (Predeterminado), De lo contrario puede escribir N y saltar al Paso 20

Paso 19. Puede cambiar el número de puerto HTTPS predeterminado de la GUI nueva de 6443 a cualquier número de puerto que desee, siempre y cuando no haya conflictos de puertos, pulse Intro para utilizar el puerto

		predeterminado (TCP/6443). Paso 20. La interfaz de administración SWA utiliza el certificado de demostración de Cisco. Escriba Y para aceptar el certificado de demostración. Puede cambiar el certificado de GUI después de la configuración inicial. Paso 21. Presione Enter para salir del asistente ifconfig.  Imagen - Nueva configuración TCP de GUI
	Configurar puerta de enlace predeterminada	Paso 22. Ejecute setgateway. Paso 23. Elija IPv4 si la interfaz de gestión se ha configurado con IPv4; de lo contrario, seleccione IPv6. Paso 24. Introduzca la dirección IP predeterminada del gateway. Paso 25. Guarde los cambios ejecutando commit. Paso 26. (Opcional) Puede agregar notas sobre los cambios que está guardando Paso 27. (Opcional) Puede disponer de SWA para realizar una copia de seguridad de la configuración antes de aplicar los cambios.

		 Imagen: Configuración de la puerta de enlace predeterminada
SSH	Importar licencia tradicional	 Nota: Si utiliza Smart License, vaya directamente al paso 36. Paso 28. Conéctese a SWA a través de SSH. Paso 29. Ejecute loadlicense Paso 30. Elija Pegar vía CLI. Paso 31. Abra el archivo de licencia con un editor de texto y copie todo su contenido Paso 32. Pegue la licencia en el shell de SSH. Paso 33. Pulse Intro para desplazarse a una nueva línea.

		Paso 34. Mantenga pulsado Control y pulse D. Paso 35. Lea el acuerdo de licencia y escriba YES para aceptar las condiciones.  Imagen - Importar licencia tradicional Vaya al paso 58.
GUI	Configurar servidor DNS	Paso 37. Inicie sesión en la GUI (el valor predeterminado es HTTPS://<FQDN de SWA o dirección IP>:8443) Paso 38. Navegue hasta Red y elija DNS. Paso 39. Haga clic en Edit Settings. Paso 40. en la sección Primary DNS Servers, seleccione Use these DNS Servers. Paso 41. Establezca la Prioridad en 0 e introduzca la dirección IP del servidor DNS.



Nota: Puede agregar más de un servidor DNS seleccionando Agregar fila.

Paso 42. Enviar.

Paso 43. Realice los cambios.

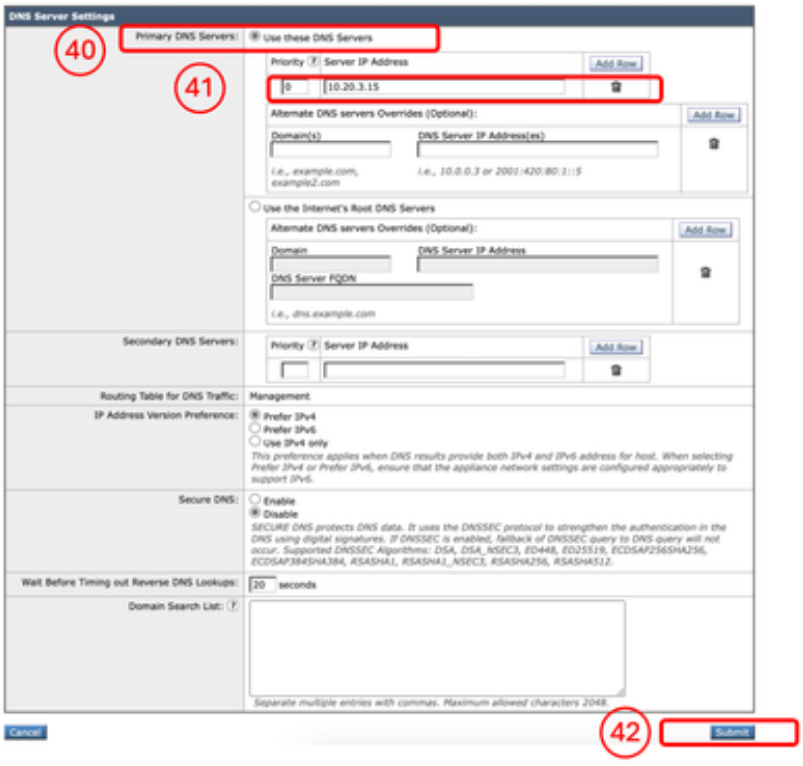
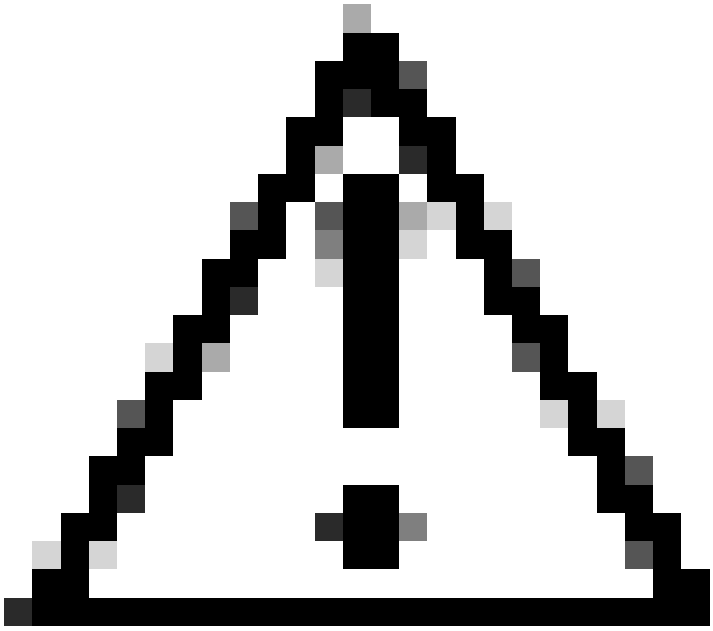


Imagen - Configurar servidor DNS

	Configurar Smart License	Paso 44. En la GUI de Administración del sistema, elija Licencias de software inteligente. Paso 45. Elija EnableSmart Software Licensing.  Precaución: no puede revertir de Smart License a Classic License, después de habilitar la función Smart License en su dispositivo. Paso 46. Haga clic en Aceptar para continuar configurando Smart License. Paso 47. Realice los cambios. Paso 48. Para obtener el token para registrar su SWA, inicie sesión en Cisco Software Central (https://software.cisco.com/#) Paso 49. Haga clic en Administrar licencias.

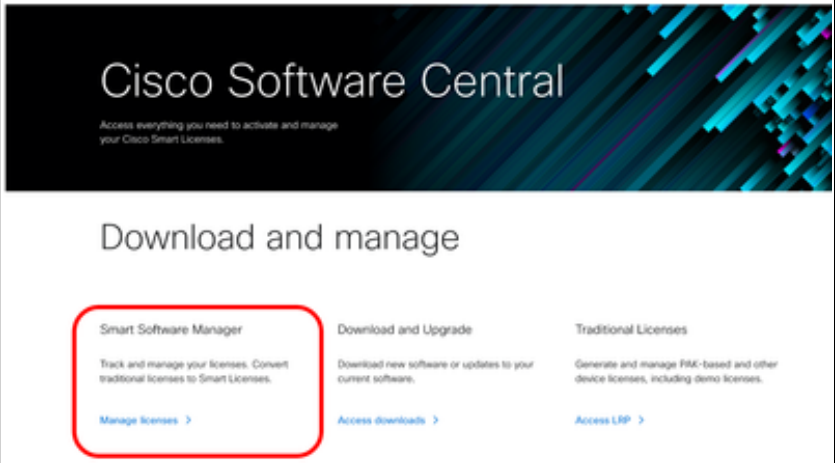


Imagen: Cisco Smart License Management

Paso 50. En Smart Software Licensing elija Inventory.

Paso 51. En la ficha General, cree un nuevo token o utilice los tokens disponibles.

Imagen - Página de inventario de licencias de Smart Software

Paso 52. Ingrese la información necesaria y Create Token.

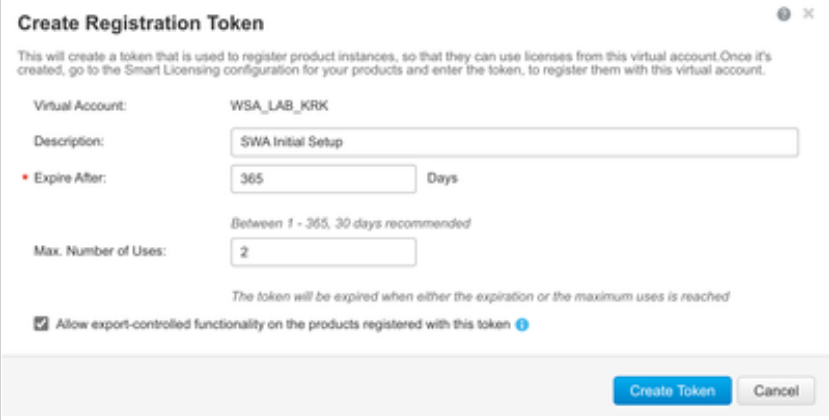
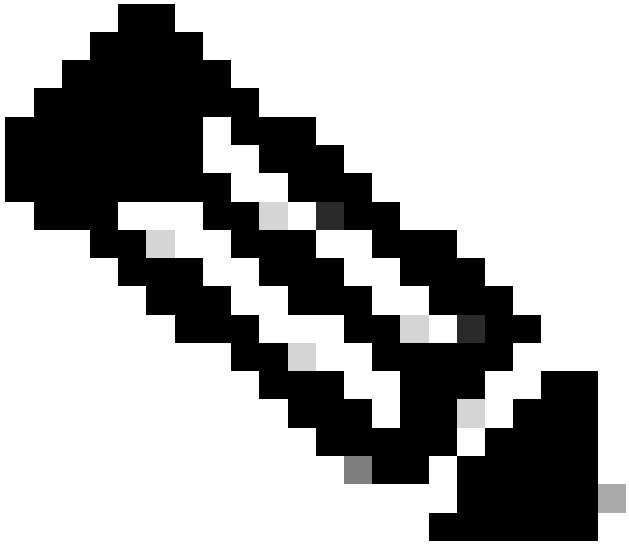


Imagen - Generación de un token

Paso 53. Haga clic en el icono azul frente al token recién agregado y copie su contenido.

Imagen - Copia del token

Paso 54. En la GUI de SWA, navegue hasta Administración del sistema y elija Licencias de software inteligente.



Nota: si ya se encuentra en la página Smart Software Licensing, actualice la página.

Paso 55. (Opcional) Si el SWA no tiene acceso a Internet desde la interfaz de administración, puede cambiar la interfaz de prueba por las interfaces que tienen permiso para acceder a Internet.

Sugerencia: Para obtener más información sobre la configuración de varias interfaces y las tablas de routing, consulte la sección Configuración de red en este artículo.

Paso 56. Haga clic en Register.

Paso 57. Pegue el token y haga clic en Register.

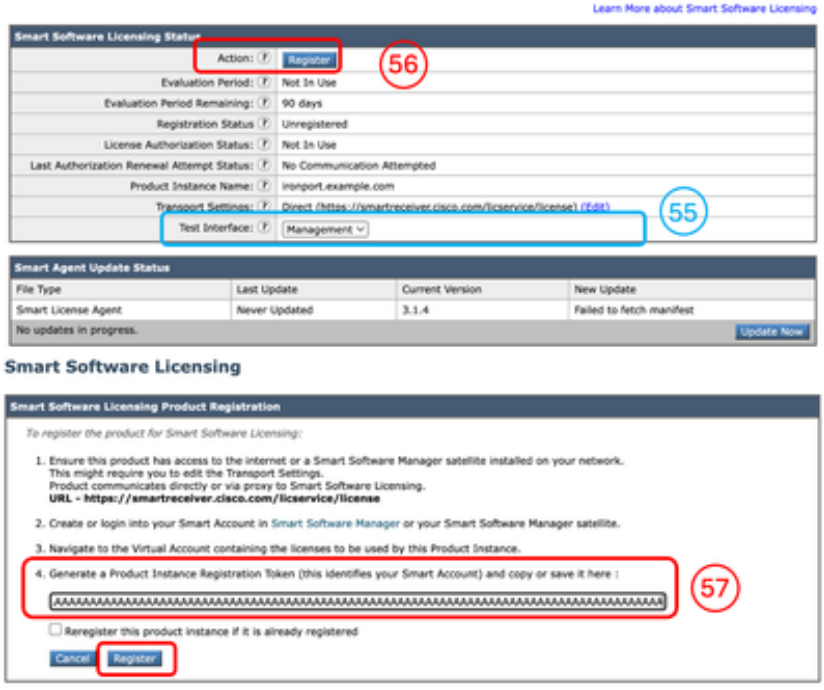
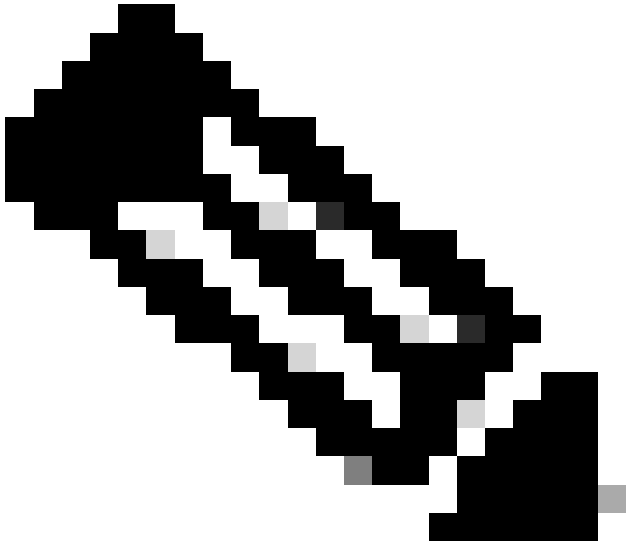
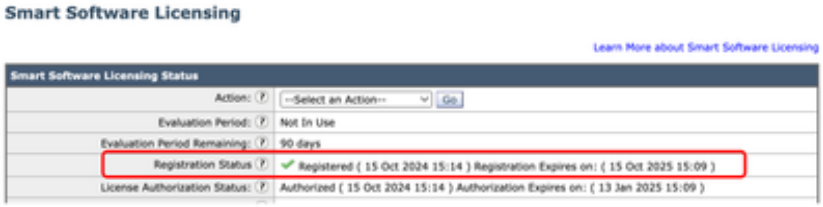
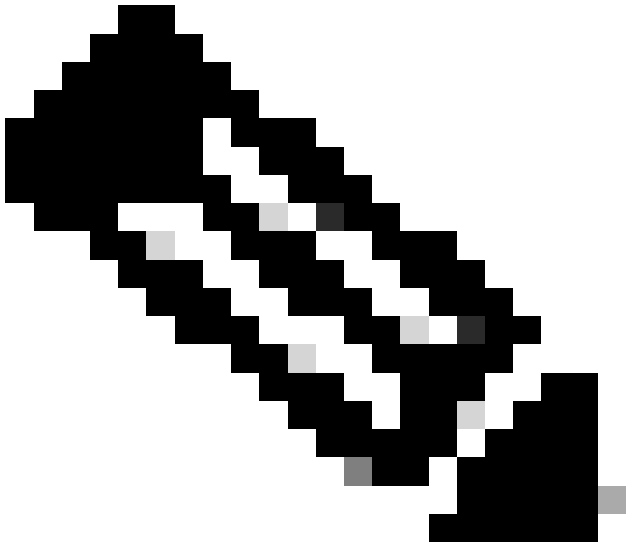


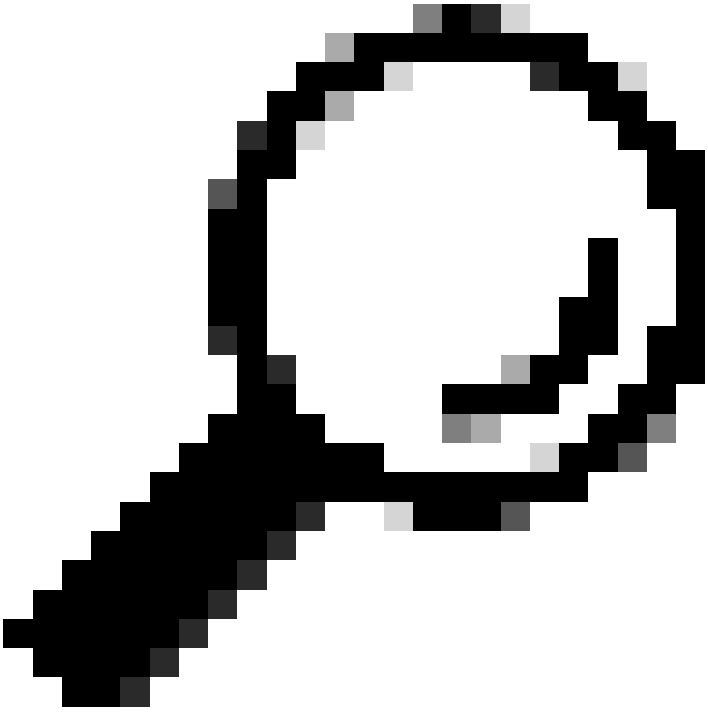
		Imagen - Registrar SWA en licencia inteligente  Nota: para verificar el registro, espere un par de minutos, actualice la página Smart Licensing en SWA y compruebe el estado del registro.  Imagen - Estado de registro de licencia inteligente
	Asistente de configuración del sistema	Paso 58. En la GUI de SWA, navegue hasta Administración del sistema y elija Asistente de configuración del sistema. Paso 59. Lea y acepte los términos de este contrato de licencia Paso 60. Haga clic en Comenzar configuración. Paso 61. Elegir Estándar de la Modo de funcionamiento del dispositivo. Paso 62. Introduzca el nombre de host predeterminado del sistema.



Nota: El nombre de host anterior que se creó en el paso 9 estaba relacionado con la interfaz de gestión y no con el SWA.

Paso 63. Introduzca la dirección IP de los servidores DNS.

Paso 64. Puede configurar el servidor de protocolo de tiempo de la red (NTP).



Sugerencia: Si el servidor NTP requiere autenticación, puede configurar los parámetros de clave.

Paso 65. Seleccione la zona horaria que se aplica al SWA y haga clic en Next.

Imagen - Asistente de configuración del sistema - Configuración del sistema

Paso 66. (Opcional) Si está utilizando cualquier Proxy upstream en su red, puede configurarlo en la página Contexto de red o bien dejarlo como predeterminado y hacer clic en Siguiente.

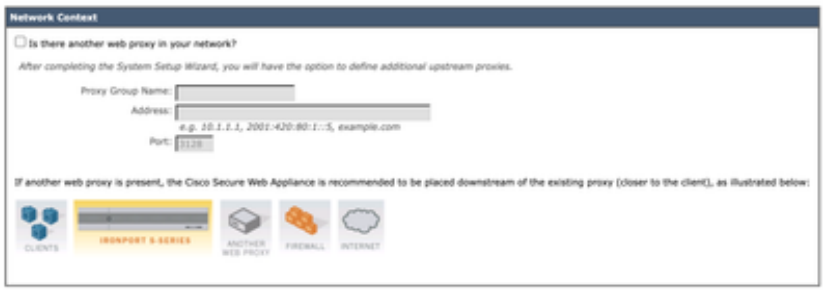
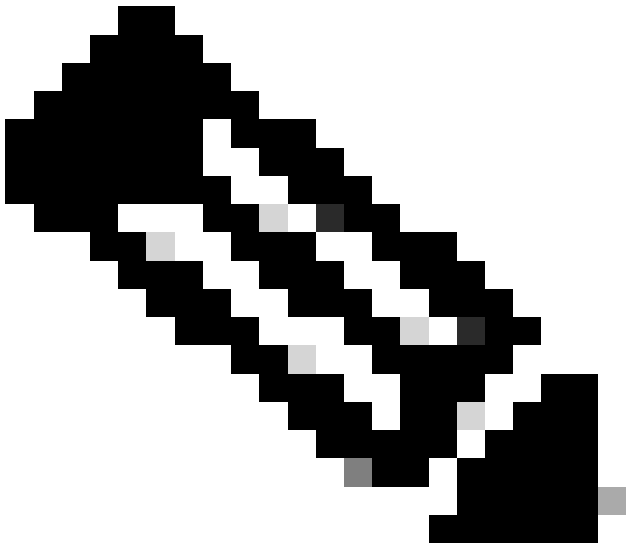


Imagen - Asistente de configuración del sistema - Configuración de proxy upstream

Paso 67. (Opcional) En caso de que necesite separar el tráfico de la interfaz de administración del tráfico de las interfaces de datos (interfaces P1 y P2), seleccione Usar puerto M1 sólo para administración.

Paso 68. (Opcional) Puede agregar o modificar la dirección IP de las interfaces de red desde la sección Dirección IPv4 / Máscara de red o Dirección IPv6 / Máscara de red.

Paso 69. (Opcional) Puede agregar o modificar el nombre de host de las interfaces de red y hacer clic en Siguiente.



Nota: El puerto P1 se puede activar y configurar mediante el asistente de configuración del sistema. Si desea activar la interfaz P2, debe hacerlo después de completar el asistente de configuración del sistema.

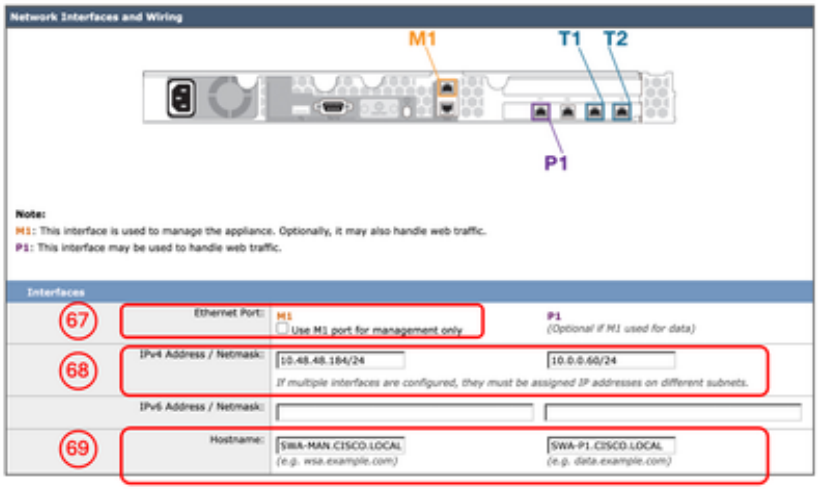


Imagen - Asistente de configuración del sistema - Configuración de interfaces de red

Paso 70. (Opcional) En caso de que esté planeando configurar el Monitor de tráfico de Capa 4 (L4TM), puede configurar el parámetro Duplex, o bien puede dejarlo como predeterminado y hacer clic en Next (Siguiente).

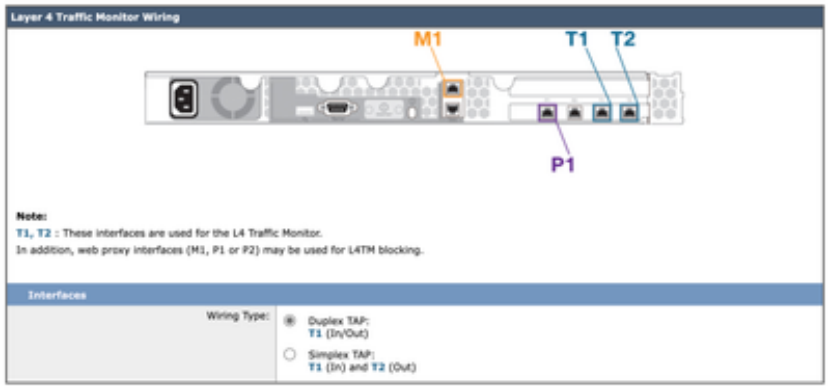
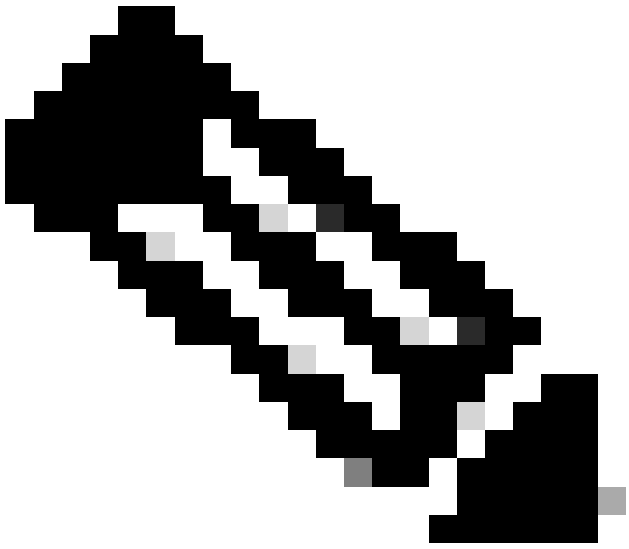


Imagen - Asistente de configuración del sistema - Configuración del monitor de tráfico de capa 4

Paso 71. (Opcional) En la página Rutas IPv4 para Gestión puede modificar la puerta de enlace predeterminada

Paso 72. (Opcional) Puede Agregar Ruta para crear Rutas Estáticas.



Nota: En caso de que elija "Usar puerto M1 solo para administración" en el paso 67, habría dos tablas de ruteo separadas para la interfaz de administración y las interfaces de datos (P1 y P2).

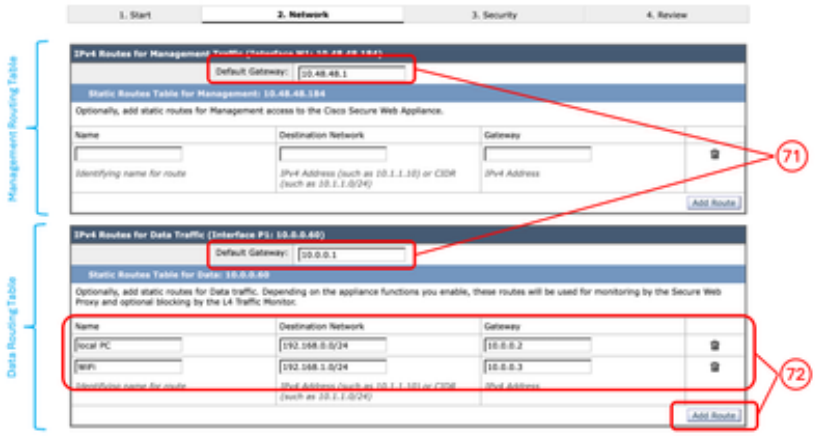


Imagen - Asistente de configuración del sistema - Agregar ruta

Paso 73. (Opcional) Si desea configurar la implementación de proxy transparente, a través del protocolo de comunicación de caché web (WCCP), puede configurar los parámetros de WCCP; de lo contrario, puede dejar el switch de capa 4 predeterminado o Sin dispositivo y hacer clic en Siguiente.

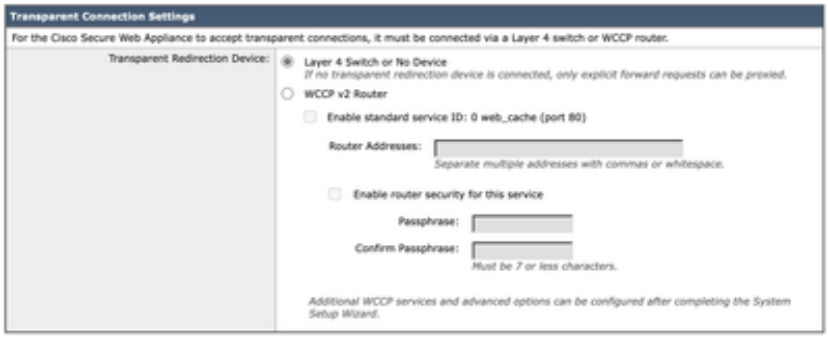


Imagen - Asistente de configuración del sistema - Configuración de implementación de proxy

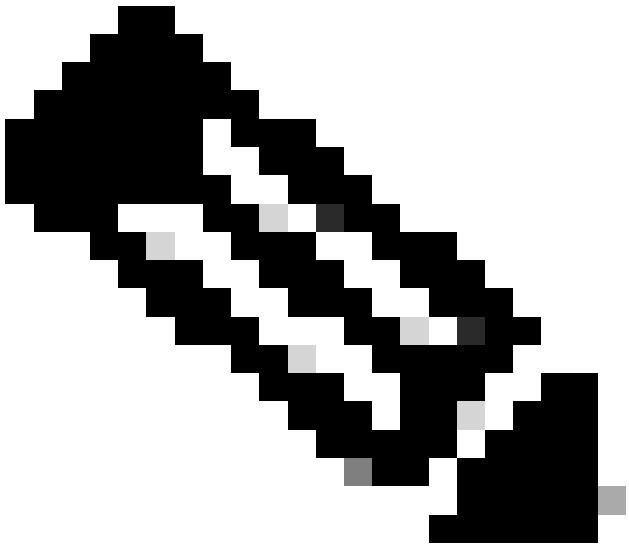
Paso 74. Configure una nueva contraseña para la cuenta de administrador.

Paso 75. Introduzca una dirección de correo electrónico que se espera que reciba alertas del sistema.

Paso 76. (Opcional) Proporcione la información del host de retransmisión de protocolo simple de transferencia de correo (SMTP); de lo contrario, déjela en blanco Si no se define ningún host de retransmisión interna, SMTP utiliza la búsqueda DNS del registro MX.

Paso 77. (Opcional) Si desea inhabilitar Participar en la red Cisco SensorBase, anule la selección de la casilla de verificación Participación de red, o bien deje la opción

predeterminada y haga clic en Siguiente.



Nota: la participación en la red Cisco SensorBase significa que Cisco recopila datos y comparte esa información con la base de datos de gestión de amenazas SensorBase.

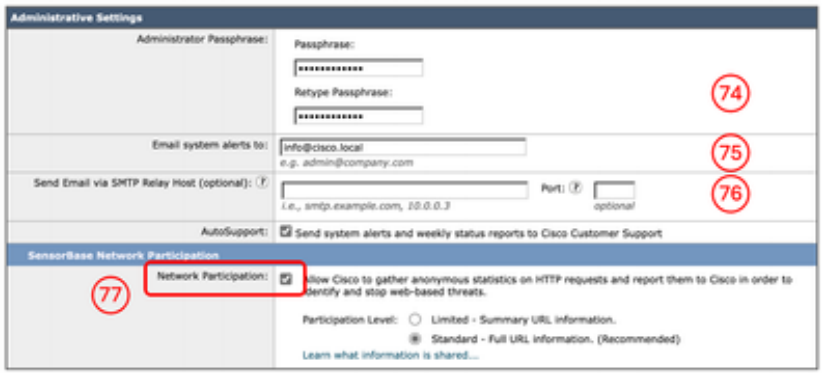


Imagen - Asistente de configuración del sistema - Configuración administrativa

Paso 78. (Opcional) Puede cambiar las acciones predeterminadas para Política global, L4TM y Filtrado de seguridad de datos de Cisco, o puede dejarlas como predeterminadas y hacer clic en Siguiente.

		Imagen - Asistente de configuración del sistema - Configuración de seguridad Paso 79. Revise la configuración. Si necesita realizar cambios, haga clic en el botón Previous para volver a la página anterior, o bien haga clic en Install This Configuration.

Configuración de red

Para configurar la interfaz de red, puede utilizar tanto CLI como GUI.

	Comando / Ruta	Acción
Configurar tarjetas de interfaz de red desde CLI	CLI > ifconfig	Nuevo: Si la interfaz no aparece en la salida de ifconfig, pero existe en la máquina virtual o el dispositivo físico, puede utilizar este comando para mostrar la interfaz en la lista. Edit: esta acción sirve para editar la dirección IP, la máscara de subred, el nombre de host de la interfaz u otros parámetros relacionados. Details: muestra detalles de una interfaz, como la dirección MAC, el tipo de medio, el modo dúplex, etc. Eliminar: Elimina la interfaz de la lista ifconfig y elimina la dirección IP si se ha asignado previamente.
Configuración de tarjetas de interfaz de red desde la GUI	GUI > Red > Interfaces	Puede editar la dirección IP y el nombre de host de la interfaz. Puede activar, desactivar o modificar el número de puerto del Servicios de gestión de

		dispositivos como FTP, SSH, acceso HTTP y acceso HTTPS.

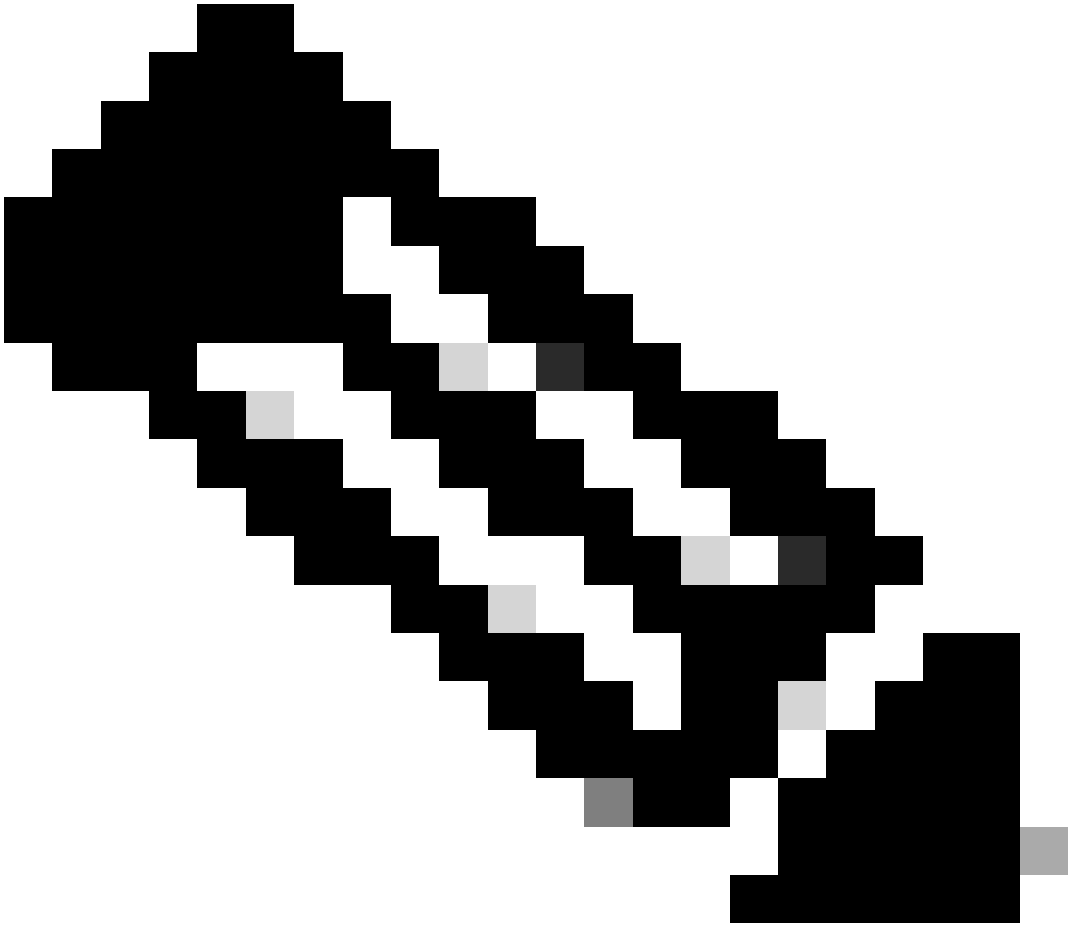
Tabla de ruteo

Las rutas son esenciales para determinar hacia dónde dirigir el tráfico de red. El SWA maneja estos tipos de tráfico:

- Tráfico de datos: Incluye el tráfico procesado por el proxy de Web de los usuarios finales que navegan por Internet.
- Tráfico de gestión: Incluye el tráfico generado por la gestión del dispositivo a través de la interfaz web, así como el tráfico para servicios de gestión como actualizaciones SWA, actualizaciones de componentes, DNS, autenticación y otras tareas relacionadas.

De forma predeterminada, ambos tipos de tráfico utilizan las rutas definidas para todas las interfaces de red configuradas. Sin embargo, tiene la opción de separar el routing de modo que el tráfico de gestión utilice una tabla de routing de gestión dedicada y el tráfico de datos utilice una tabla de routing de datos independiente.

Tráfico de gestión	Tráfico de datos
WebUI SSH SNMP (Protocolo de administración de red simple) Autenticación, con controlador de dominio (configurable) Registros del sistema FTP push DNS (configurable) Actualización/actualización/clave de característica (configurable)	Proxy HTTP Proxy HTTPS Proxy FTP negociación WCCP Solicitud ICAP con servidor DLP externo DNS (configurable) Actualización/actualización/clave de característica (configurable) Autenticación con controlador de dominio (configurable)



Nota: Si selecciona la opción "Usar puerto M1 solo para administración", se agregará al SWA una tabla de routing adicional denominada tabla de routing de datos. Esta tabla de routing solo tiene un gateway predeterminado configurable; las rutas de routing adicionales deben configurarse manualmente.

Información Relacionada

- Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance
- Guía de instalación de Cisco Secure Email and Web Virtual Appliance
- Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco
- Uso de las prácticas recomendadas de Secure Web Appliance
- Configuración del firewall para el dispositivo web seguro
- Configurar certificado de descifrado en dispositivo web seguro

- Configuración y solución de problemas de SNMP en SWA
- Configuración de registros de inserción de SCP en un dispositivo web seguro con Microsoft Server
- Habilitar canal/vídeo específico de YouTube y bloquear el resto de YouTube en SWA
- Comprensión del formato de registro de acceso HTTPS en el dispositivo web seguro
- Acceder a registros de appliances web seguros
- Omitir autenticación en dispositivo web seguro
- Bloqueo del tráfico en el dispositivo web seguro
- Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).