

Configurar a configuração inicial do Secure Web Appliance

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Instalação do SWA](#)

[Configuração inicial](#)

[Configurar endereço IP](#)

[Configurar gateway padrão](#)

[Importar licença tradicional](#)

[Configurar servidor DNS](#)

[Configurar Smart License](#)

[Assistente de configuração do sistema](#)

[Configuração de rede](#)

[Routing Table](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas necessárias para configurar o Secure Web Appliance (SWA) pela primeira vez.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.
- Princípios fundamentais de rede.

A Cisco recomenda que você:

- SWA físico ou virtual instalado.
- Acesso administrativo à interface gráfica do usuário (GUI) do SWA.
- Acesso administrativo à interface de linha de comando (CLI) do SWA.
- Acesso administrativo ao console SWA.
- Licença SWA válida ou acesso ao portal de gerenciamento de licenças inteligentes (caso

você esteja usando a Licença inteligente).

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Instalação do SWA

O Cisco SWA é uma solução proxy avançada projetada para aprimorar a segurança e o controle da Web para as empresas. Disponível em formatos virtuais e físicos, o SWA oferece opções de implantação flexíveis para atender a diversas necessidades. O SWA virtual suporta várias plataformas de hipervisor, incluindo Microsoft Hyper-V, VMware ESX e KVM, garantindo a compatibilidade com uma variedade de ambientes virtuais. Para aqueles que preferem um dispositivo físico, a Cisco oferece três modelos distintos: S100, S300 e S600. Cada modelo é projetado para atender a diferentes níveis de desempenho e requisitos de capacidade, garantindo que as empresas possam encontrar a opção certa para suas necessidades específicas de segurança na Web.

Para fazer download da imagem da sua máquina virtual, acesse:

<https://software.cisco.com/download/home> .

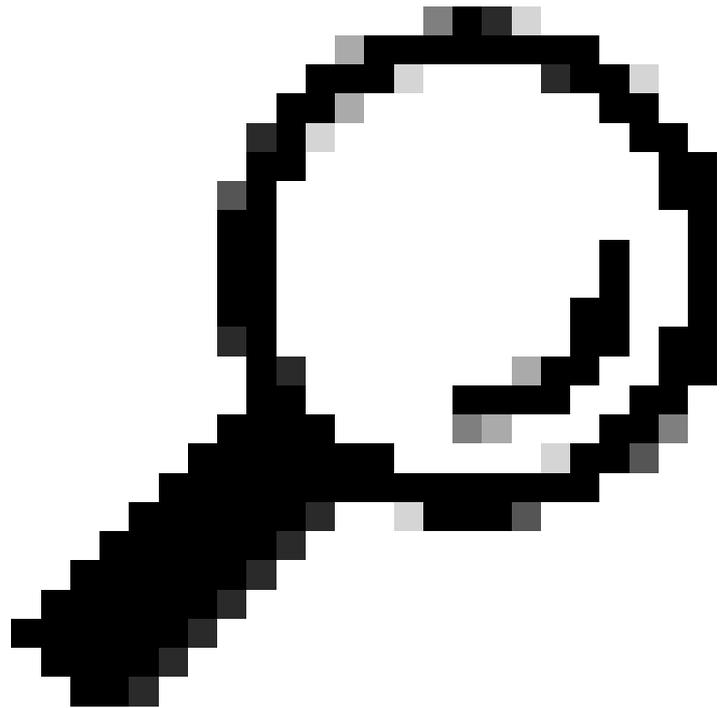
A instalação do Cisco SWA virtual é um processo simples que começa com a seleção da plataforma de hipervisor apropriada. Primeiro, faça o download do arquivo de instalação virtual do SWA no site da Cisco. Para o VMware ESX, implante o arquivo OVA, garantindo que você defina as configurações de rede e aloque recursos suficientes, como CPU, memória e armazenamento. Para o Microsoft Hyper-V, importe o arquivo VHD baixado para o Gerenciador do Hyper-V e defina as configurações da máquina virtual de acordo. Para KVM, use a ferramenta de linha de comando virt-manager ou virsh para definir e iniciar a máquina virtual usando a imagem baixada. Quando a máquina virtual estiver em execução, você poderá usar as etapas deste artigo para fazer a configuração inicial.

Configuração inicial

Após instalar o SWA, continue com estas etapas para a implantação inicial.

Observação: para a configuração inicial, você precisa ter acesso ao SWA via Console, SSH e GUI.

Método de conexão	Estágio	Configuration Steps
Console	Configurar endereço IP	Etapa 1. Digite o nome de usuário e a senha para fazer login na CLI.



Dica: o nome de usuário padrão é admin e a senha padrão é ironport.

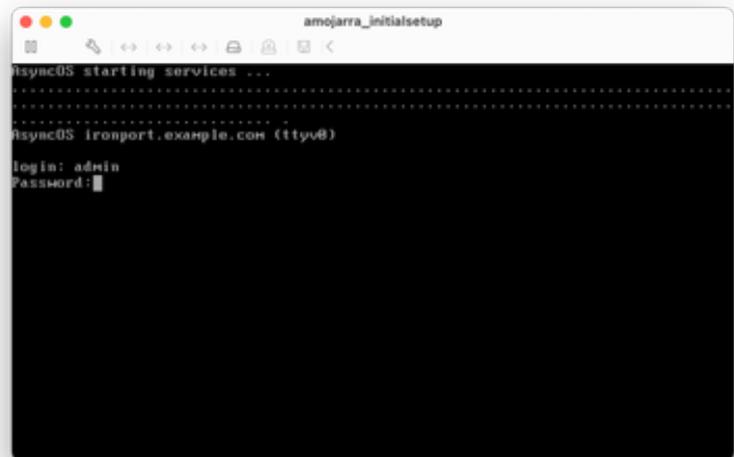


Imagem - Tela de login

Etapa 2. Execute ifconfig.

Etapa 3. Escolha Editar.

Etapa 4. Insira o número associado à sua interface de gerenciamento.

Etapa 5. Selecione Y para editar o endereço IPv4 padrão.

Etapa 6. Insira o endereço IP

Passo 7. Insira a Máscara de sub-rede.

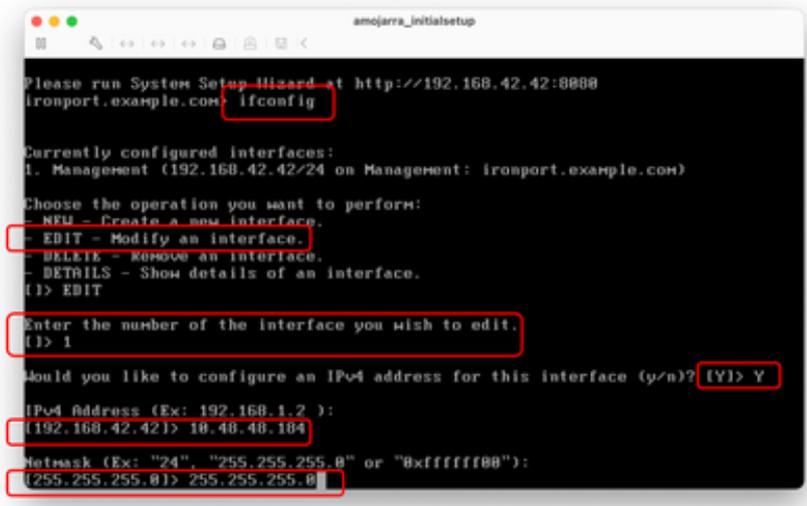


Imagem - Editar endereço IP da interface de gerenciamento

Etapa 8. Se você quiser configurar o IPv6, digite Y em resposta à pergunta "Você gostaria de configurar o IPv6?"; caso contrário, você pode deixar como padrão (No) e pressionar Enter.

Etapa 9. Insira um nome de domínio totalmente qualificado (FQDN) como o nome do host.

Etapa 10. Se quiser habilitar o acesso ao protocolo de transferência de arquivos (FTP) à interface de gerenciamento, escolha Y ou pressione Enter.

Etapa 11. O Shell Seguro (SSH) é definido como Habilitado por padrão. Recomenda-se que o SSH esteja habilitado. Digite Y para continuar.

Etapa 12. (Opcional) Você pode alterar a porta SSH padrão de TCP 22 para qualquer número de porta desejado, desde que não haja conflitos de porta ou pressione enter para usar a porta padrão (TCP/22).

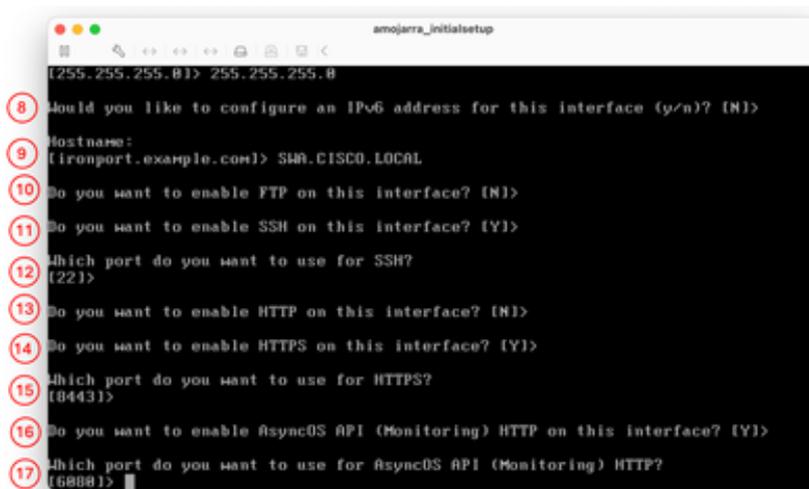
Etapa 13. Se você quiser ter acesso ao protocolo HTTP à interface de gerenciamento, digite Y e defina o número da porta para acesso HTTP. Caso contrário, você pode escolher N para ter acesso somente ao protocolo HTTPS à interface de gerenciamento.

Etapa 14. Digite Y e pressione Enter para habilitar o acesso HTTPS à Interface de Gerenciamento.

Etapa 15. Você pode alterar o número de porta HTTPS padrão de 8443 para qualquer número de porta desejado, desde que não haja conflitos de porta ou pressione Enter para usar a porta padrão (TCP/8443).

Etapa 16. Por padrão, a API (Application Programming Interface, Interface de programação de aplicativos) está definida como Habilitar. Se você não estiver usando a API, poderá desabilitá-la digitando N e pressionando Enter.

Etapa 17. Se você optar por ativar a API, poderá alterar o número da porta da API padrão de 6080 para qualquer número de porta desejado, desde que não haja conflitos de porta ou pressione Enter para usar a porta padrão (TCP/6080).



```
amojara_initialsetup
[255.255.255.0] 255.255.255.0
(8) Should you like to configure an IPv6 address for this interface (y/n)? [N]
(9) Hostname:
[ironport.example.com] SW1.CISCO.LOCAL
(10) Do you want to enable FTP on this interface? [N]
(11) Do you want to enable SSH on this interface? [Y]
(12) Which port do you want to use for SSH?
[22]
(13) Do you want to enable HTTP on this interface? [N]
(14) Do you want to enable HTTPS on this interface? [Y]
(15) Which port do you want to use for HTTPS?
[8443]
(16) Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [Y]
(17) Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6080]
```

Imagem - Configuração do Serviço de Interface de Gerenciamento

Etapa 18. AsyncOS API (monitoramento) é a nova GUI no SWA. Se você quiser usar os novos relatórios de interface de usuário, defina esta opção como Y (Padrão). Caso contrário, você pode digitar N e ir para a Etapa 20

Etapa 19. Você pode alterar o número da porta padrão New GUI HTTPS de 6443 para qualquer número de porta desejado, desde que não haja conflitos de porta ou pressione Enter para usar a porta padrão (TCP/6443).

Etapa 20. A interface de gerenciamento SWA usa o certificado de demonstração Cisco. Digite Y para aceitar o certificado de demonstração. você pode alterar o certificado da GUI após a configuração inicial.

Etapa 21. Pressione Enter para sair do assistente ifconfig.

```
amojarra_initialsetup
Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [Y]
Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6888]
18 Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [Y]
19 Which port do you want to use for AsyncOS API (Monitoring) HTTPS?
[6443]
20 You have not entered an HTTPS certificate. To assure privacy, run "certconfig"
first. You may use the demo, but this will not be secure.
Do you really wish to use a demo certificate? [Y]

Currently configured interfaces:
1. Management (18.48.48.184/24 on Management: SWA.CISCO.LOCAL)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
21 [1] >
```

Imagem - Nova configuração de TCP da GUI

Configurar gateway padrão

Etapa 22. Execute setgateway.

Etapa 23. Escolha o IPv4 se sua interface de gerenciamento tiver sido configurada com IPv4, caso contrário, escolha IPv6.

Etapa 24. Insira o endereço IP do gateway padrão.

Etapa 25. Salve as alterações executando commit.

Etapa 26. (Opcional) você pode adicionar Observações sobre as alterações que está salvando

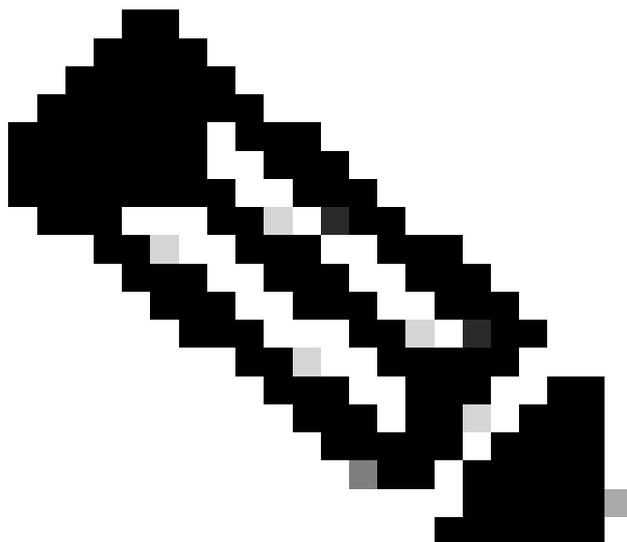
Etapa 27. (Opcional) Você pode fazer com que o SWA faça backup da configuração antes de aplicar as alterações.

```
amojarra_initialsetup
Please run System Setup Wizard at http://18.48.48.184:8888
(ironport.example.com) setgateway
Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Set the default gateway for:
22 [1] >
23 1. IPv4
2. IPv6
[1] > 1
Enter new default gateway:
24 [18.48.48.254] > 18.48.48.1
Please run System Setup Wizard at http://18.48.48.184:8888
25 (ironport.example.com) commit
Please enter some comments describing your changes:
[1] >
Do you want to save the current configuration for rollback? [Y]
27 Changes committed: Tue Oct 15 12:33:59 2024 GMT
Please run System Setup Wizard at http://18.48.48.184:8888
(ironport.example.com) >
```

Imagem - Configurando o gateway padrão

SSH

Importar licença tradicional



Observação: se você estiver usando a Smart License, vá para a etapa 36.

Etapa 28. Conecte-se ao SWA via SSH.

Etapa 29. Executar loadlicense

Etapa 30. Escolha Colar via CLI.

Etapa 31. Abra o arquivo de licença com um editor de texto e copie todo o seu conteúdo

Etapa 32. Cole a licença no shell SSH.

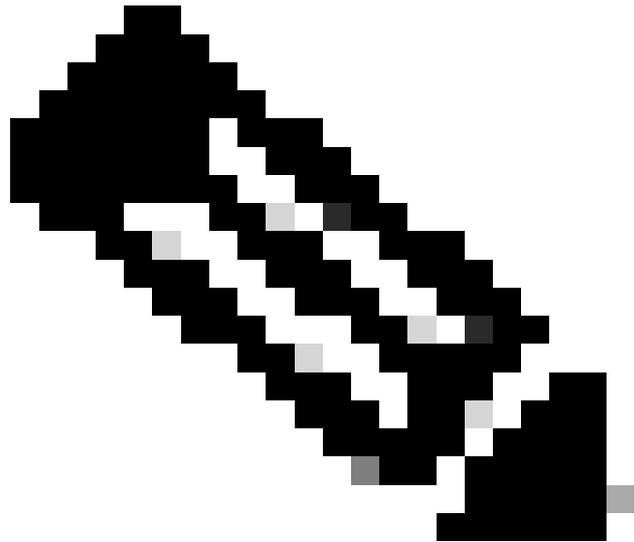
Etapa 33. Pressione Enter para navegar para uma nova linha.

Etapa 34. Mantenha Control pressionado e pressione D.

Etapa 35. Leia o Contrato de licença e digite YES para concordar com as condições.

		 <p>Imagem - Importar licença tradicional</p> <p>Vá para a Etapa 58.</p>
--	--	--

GUI	Configurar servidor DNS	<p>Etapa 37. Faça login na GUI (o padrão é HTTPS://<SWA FQDN or IP Address>:8443)</p> <p>Etapa 38. Navegue até Network e escolha DNS.</p> <p>Etapa 39. Clique em Edit Settings.</p> <p>Etapa 40. na seção Servidores DNS primários, selecione Usar estes servidores DNS.</p> <p>Etapa 41. Defina a Prioridade como 0 e insira o endereço IP do servidor DNS.</p>
-----	-------------------------	--



Observação: você pode adicionar mais de um servidor DNS escolhendo Adicionar linha.

Etapa 42. Enviar.

Etapa 43. Confirme as alterações.

DNS Server Settings

Primary DNS Servers: Use these DNS Servers

Priority	Server IP Address	Add Row
0	10.20.3.15	

Alternate DNS servers Overrides (Optional):

Domain(s)	DNS Server IP Address(es)	Add Row

Alternate DNS servers Overrides (Optional):

Domain	DNS Server IP Address	Add Row

Secondary DNS Servers:

Priority	Server IP Address	Add Row

Routing Table for DNS Traffic:

IP Address Version Preference:

Management:

Secure DNS:

Wait Before Timing out Reverse DNS Lookups:

Domain Search List:

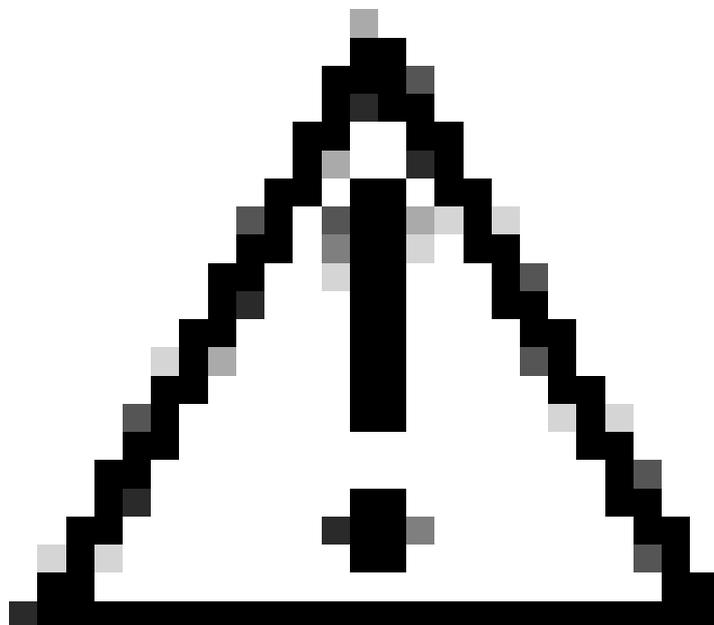
Cancel 42 Submit

Imagem - Configurar servidor DNS

Configurar Smart License

Etapa 44. Na GUI em Administração do sistema, escolha Licenciamento de software inteligente.

Etapa 45. Selecione EnableSmart Software Licensing.



Cuidado: não é possível reverter de Licença inteligente para Licença clássica, depois de habilitar o recurso Licença inteligente no seu dispositivo.

Etapa 46. Clique em OK para continuar configurando a Smart License.

Etapa 47. Confirme as alterações.

Etapa 48. Para obter o token para registrar seu SWA, faça login na Cisco Software Central (<https://software.cisco.com/#>)

Etapa 49. Clique em Gerenciar licenças.



Download and manage

Smart Software Manager
Track and manage your licenses. Convert traditional licenses to Smart Licenses.
[Manage licenses >](#)

Download and Upgrade
Download new software or updates to your current software.
[Access downloads >](#)

Traditional Licenses
Generate and manage PKM-based and other device licenses, including demo licenses.
[Access LRP >](#)

Imagem - Cisco Smart License Management

Etapa 50. Em Smart Software Licensing, escolha Inventory.

Etapa 51. Na guia Geral, crie um novo token ou use seus tokens disponíveis.



Imagem - Página de inventário de licenças de software inteligente

Etapa 52. Insira as informações necessárias e Create Token.

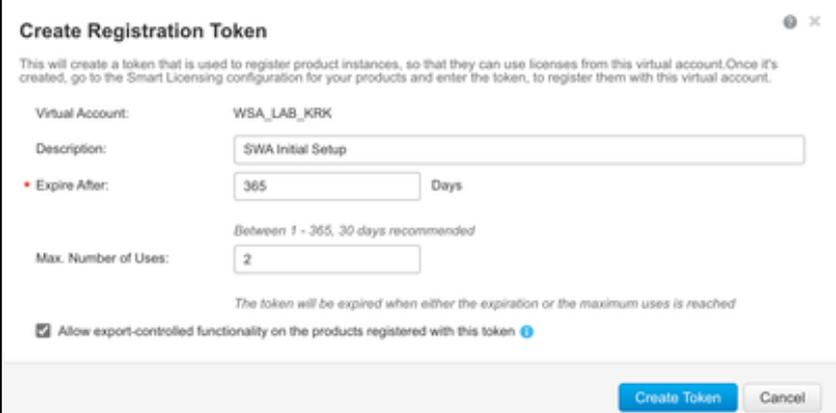


Imagem - Gerando um token

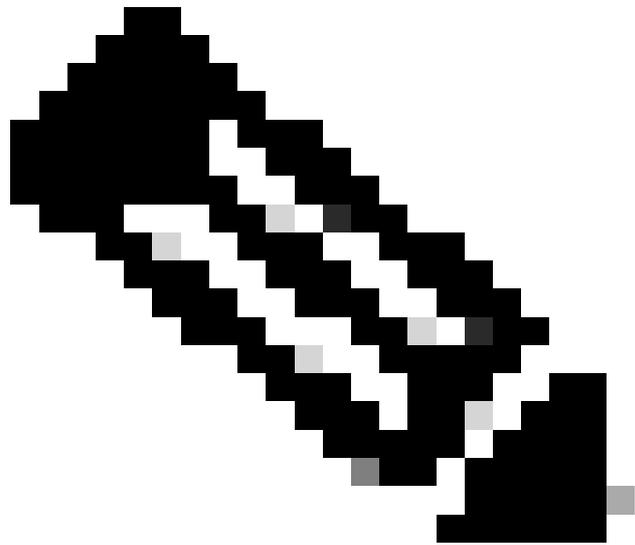
Etapa 53. Clique no ícone azul na frente do token recém-

adicionado e copie seu conteúdo.



Imagem - Copiar o token

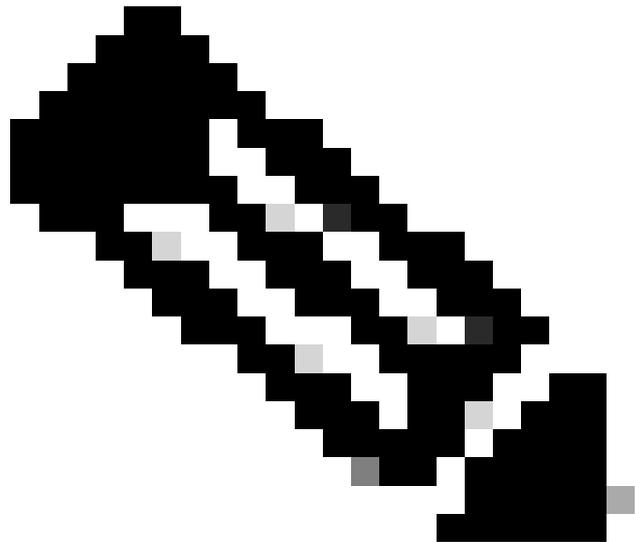
Etapa 54. Na GUI do SWA, navegue para System Administration e escolha Smart Software Licensing.



Observação: se você já estiver na página Smart Software Licensing, atualize a página.

Etapa 55. (Opcional) Se o SWA não tiver acesso à Internet a partir da interface de gerenciamento, você poderá alterar a interface de teste para as interfaces que têm permissão para acessar a Internet.

Imagem - Registrar SWA na Smart License



Observação: para verificar seu registro, aguarde alguns minutos, atualize a página Smart Licensing no SWA e verifique o Registration Status.

Smart Software Licensing

[Learn More about Smart Software Licensing](#)

Smart Software Licensing Status	
Action:	--Select an Action-- <input type="button" value="Go"/>
Evaluation Period:	Not In Use
Evaluation Period Remaining:	90 days
Registration Status:	✓ Registered (15 Oct 2024 15:14) Registration Expires on: (15 Oct 2025 15:09)
License Authorization Status:	Authorized (15 Oct 2024 15:14) Authorization Expires on: (13 Jan 2025 15:09)

Imagem - Status de registro da Smart License

Assistente de configuração do sistema

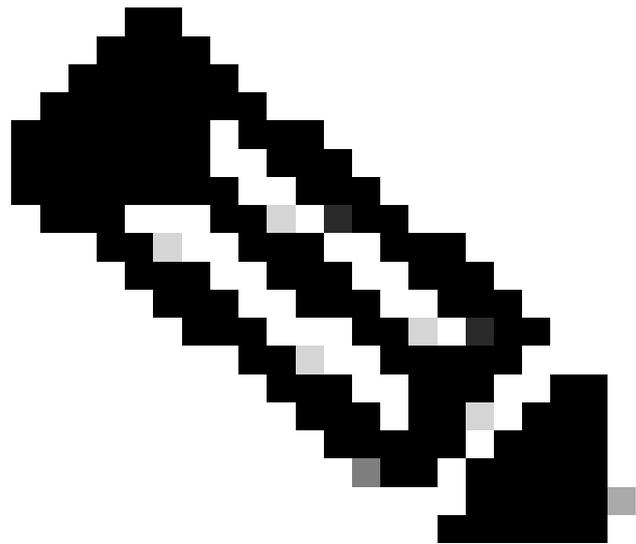
Etapa 58. Na GUI do SWA, navegue para Administração do sistema e escolha Assistente de configuração do sistema.

Etapa 59. Leia e aceite os termos deste contrato de licença

Etapa 60. Clique em Begin Setup.

Etapa 61. Escolha Padrão do Seção Modo de operação do dispositivo.

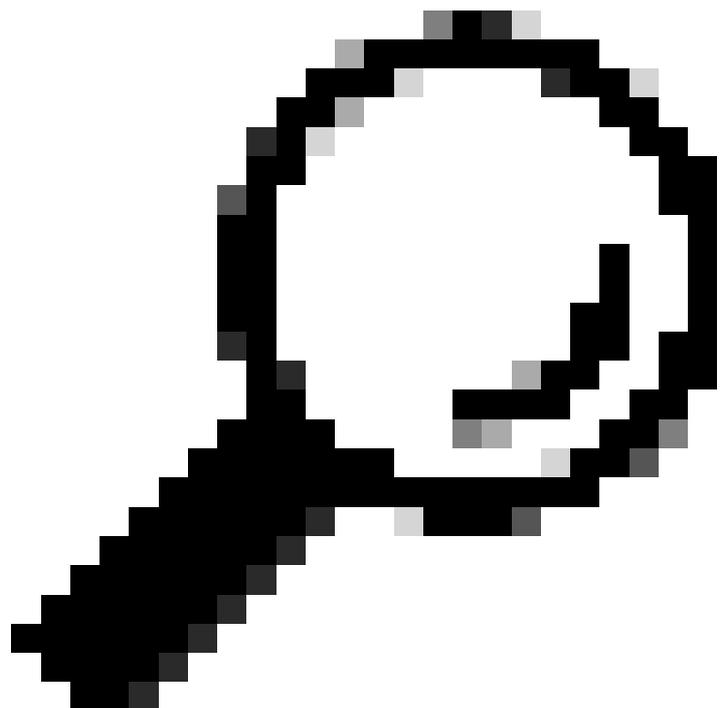
Etapa 62. Insira o nome de host do sistema padrão.



Observação: o nome de host anterior criado na Etapa 9 estava relacionado à interface de gerenciamento e não ao SWA.

Etapa 63. Insira o endereço IP do servidor(es) DNS.

Etapa 64. você pode configurar seu servidor Network Time Protocol (NTP).



Dica: se o servidor NTP exigir autenticação, você

poderá configurar os parâmetros Key.

Etapa 65. Selecione o fuso horário que se aplica ao SWA e clique em Avançar.

Imagem - Assistente de configuração do sistema - Configurações do sistema

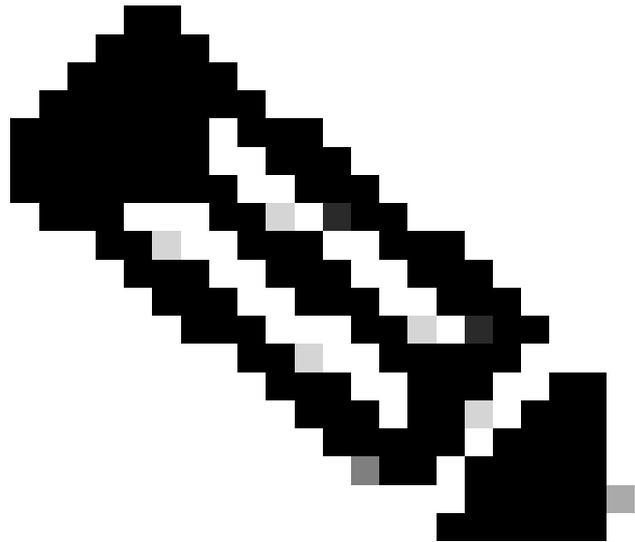
Etapa 66. (Opcional) Se estiver usando qualquer Proxy de upstream na rede, você poderá configurá-lo na página Contexto de rede ou deixá-lo como padrão e clicar em Avançar.

Imagem - Assistente de configuração do sistema - Configuração do proxy de upstream

Etapa 67. (Opcional) Caso você precise separar o tráfego da interface de gerenciamento do tráfego das interfaces de dados (interfaces P1 e P2), selecione Usar porta M1 apenas para gerenciamento.

Etapa 68. (Opcional) Você pode adicionar ou modificar o endereço IP das interfaces de rede na seção Endereço IPv4 / Máscara de rede ou Endereço IPv6 / Máscara de rede.

Etapa 69. (Opcional) Você pode adicionar ou modificar o nome de host das interfaces de rede e clicar em Avançar.



Observação: a porta P1 pode ser ativada e configurada através do Assistente de configuração do sistema. Se desejar habilitar a interface P2, isso deverá ser feito após concluir o Assistente de configuração do sistema.

Network Interfaces and Wiring			
Note: M1: This interface is used to manage the appliance. Optionally, it may also handle web traffic. P1: This interface may be used to handle web traffic.			
Interfaces			
67	Ethernet Port:	M1 <input type="checkbox"/> Use M1 port for management only	P1 (Optional if M1 used for data)
68	IPv4 Address / Netmask:	10.48.48.184/24	10.0.0.60/24
	IPv6 Address / Netmask:		
69	Hostname:	SWA-MAN.CISCO.LOCAL (e.g. wsa.example.com)	SWA-P1.CISCO.LOCAL (e.g. data.example.com)

Imagem - Assistente de configuração do sistema - Configuração de interfaces de rede

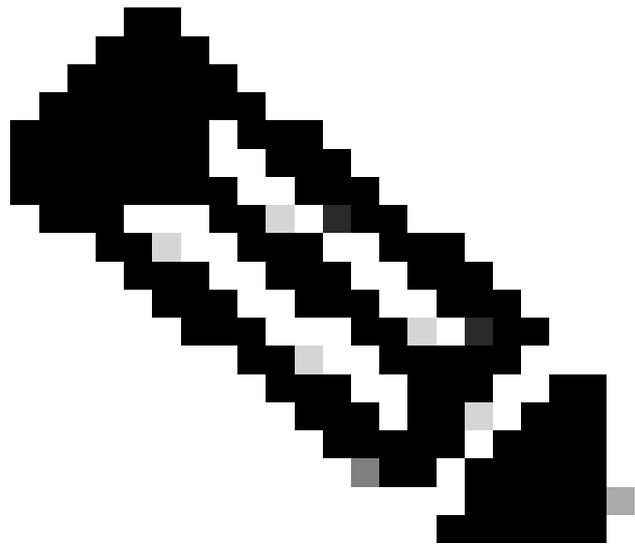
Etapa 70. (Opcional) Caso esteja planejando configurar o L4TM (Layer 4 Traffic Monitor), você pode configurar a configuração Duplex, ou então pode deixar como padrão e clicar em Avançar.



Imagem - Assistente de configuração do sistema - Configuração do monitor de tráfego de camada 4

Etapa 71. (Opcional) Na página Rotas IPv4 para gerenciamento você pode modificar o gateway padrão

Etapa 72. (Opcional) Você pode adicionar uma rota para criar rotas estáticas.



Observação: caso você escolha "Usar porta M1 somente para gerenciamento" na Etapa 67, haverá duas tabelas de roteamento separadas para a interface de gerenciamento e as interfaces de dados (P1 e P2).

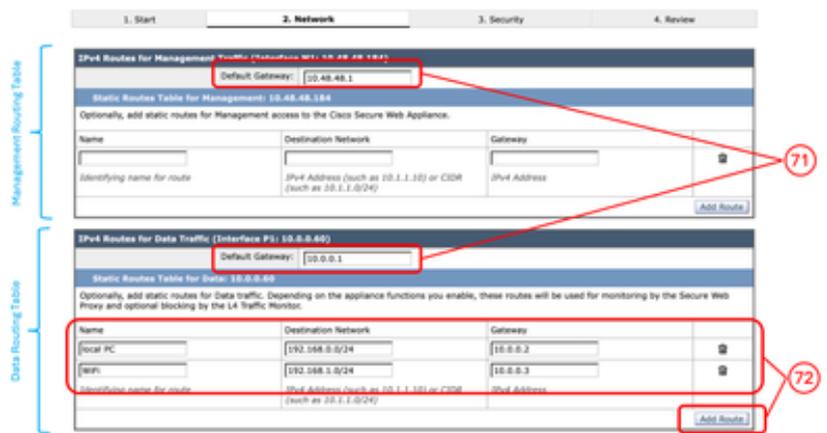


Imagem - Assistente de configuração do sistema - Adicionar rota

Etapa 73. (Opcional) Se quiser configurar a implantação do Transparent Proxy, via Web Cache Communication Protocol (WCCP), você pode definir as configurações do WCCP ou pode deixar o Layer 4 Switch ou No Device padrão e clicar em Next.

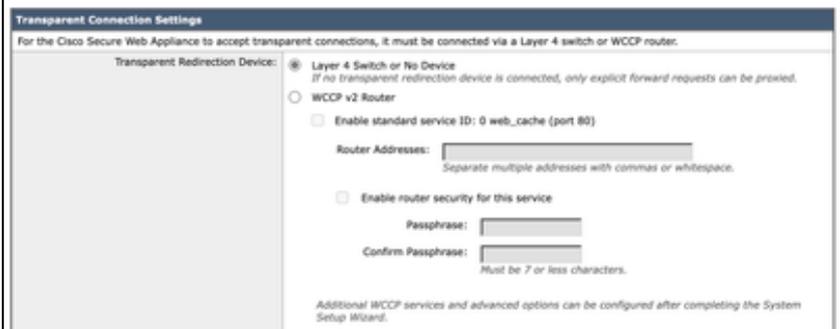


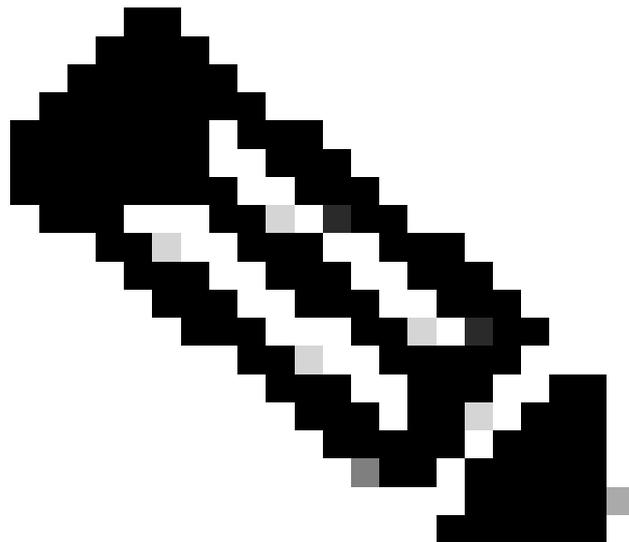
Imagem - Assistente de configuração do sistema - Configuração da implantação de proxy

Etapa 74. Configure uma nova senha para a conta de administrador.

Etapa 75. Insira um endereço de e-mail que deve receber alertas do sistema.

Etapa 76. (Opcional) Fornecer as informações do SMTP (Simple Mail Transfer Protocol) Relay host, caso contrário, deixá-las em branco. Se nenhum host de retransmissão interno estiver definido, o SMTP usará a pesquisa DNS do registro MX.

Etapa 77. (Opcional) Se você quiser desabilitar Participação na rede Cisco SensorBase, desmarque a caixa de seleção Participação de rede ou deixe como padrão e clique em Avançar.



Observação: a participação na rede Cisco SensorBase significa que a Cisco coleta dados e compartilha essas informações com o banco de dados de gerenciamento de ameaças SensorBase.

Administrative Settings

Administrator Passphrase: Passphrase: [] Retype Passphrase: []

Email system alerts to: info@cisco.local e.g. admin@company.com

Send Email via SMTP Relay Host (optional): [] Port: [] optional

AutoSupport: Send system alerts and weekly status reports to Cisco Customer Support

SensorBase Network Participation

77 Network Participation: Allow Cisco to gather anonymous statistics on HTTP requests and report them to Cisco in order to identify and stop web-based threats.

Participation Level: Limited - Summary URL information. Standard - Full URL information. (Recommended)

Learn what information is shared...

74 75 76

Imagem - Assistente de configuração do sistema - Configurações administrativas

Etapa 78. (Opcional) Você pode alterar as ações padrão para Política global, L4TM e Filtragem de segurança de dados da Cisco, ou pode deixá-las como padrão e clicar em Avançar.

Security Settings

Global Policy Default Action: Monitor all traffic Block all traffic

If block all traffic is selected, the Global Access Policy will be initially configured to block all proxied protocols (HTTP, HTTPS, FTP over HTTP, and native FTP).

L4 Traffic Monitor: Action for Suspect Malware Addresses: Monitor only Block

Cisco Data Security Filtering: Enable

The Global Cisco Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads.

		<p>Imagem - Assistente de configuração do sistema - Configurações de segurança</p> <p>Etapa 79. Revise sua configuração. Se precisar fazer alterações, clique no botão Anterior para retornar à página anterior ou clique em Instalar esta configuração.</p>
--	--	--

Configuração de rede

Para configurar a interface de rede, você pode usar a CLI ou a GUI.

	Comando/Caminho	Ação
Configurar placas de interface de rede a partir do CLI	CLI > ifconfig	<p>Novo: se a interface não estiver listada na saída ifconfig, mas existir na máquina virtual ou no dispositivo físico, você poderá usar esse comando para mostrar a interface na lista.</p> <p>Editar: esta ação serve para editar o endereço IP, a máscara de sub-rede, o nome de host da interface ou outros parâmetros relacionados.</p> <p>Detalhes: mostra detalhes de uma interface, como Endereço MAC, Tipo de Mídia, Modo Duplex e assim por diante.</p> <p>Excluir: remove a interface da lista ifconfig e remove o endereço IP, se atribuído anteriormente.</p>
Configurar placas de interface de rede a partir da GUI	GUI > Rede > Interfaces	<p>Você pode Editar o endereço IP e o nome do host da interface.</p> <p>Você pode Ativar, Desativar ou modificar o número da porta do</p> <p>Serviços de gerenciamento de dispositivos como acesso FTP, SSH, HTTP e HTTPS.</p>

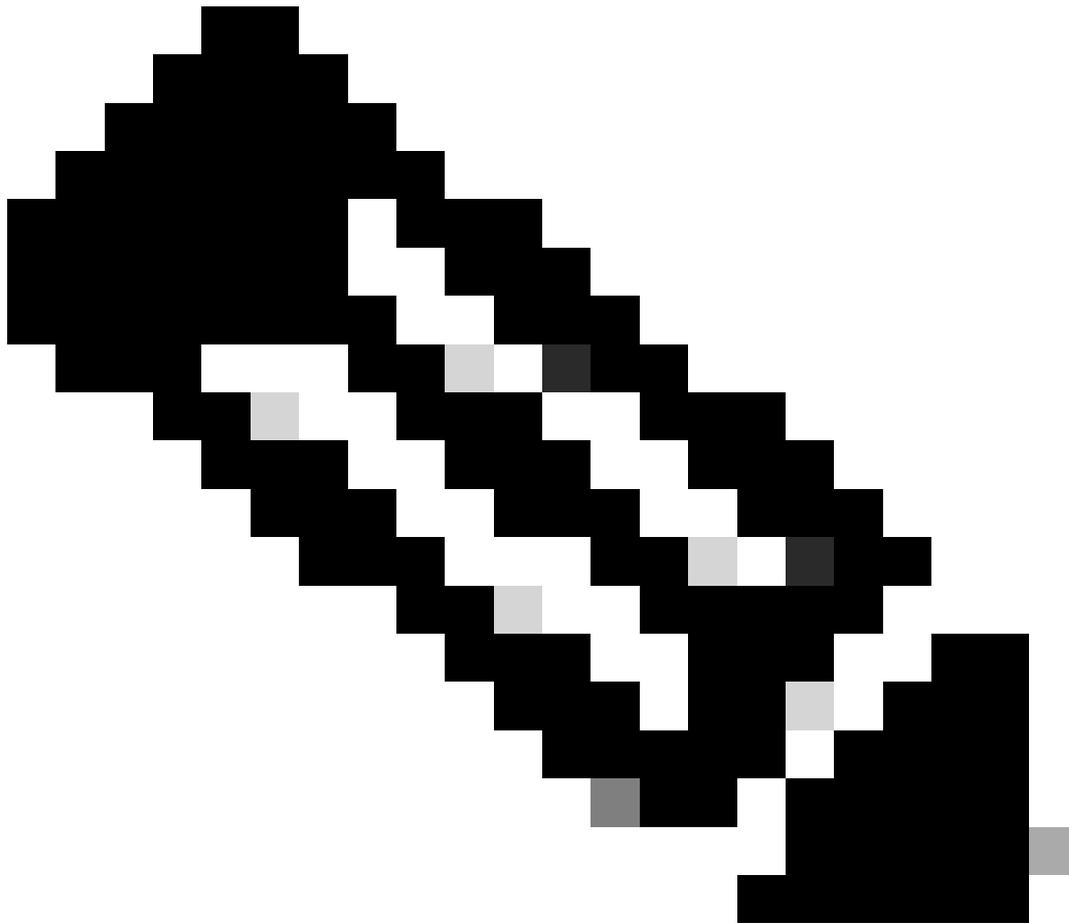
Routing Table

As rotas são essenciais para determinar para onde direcionar o tráfego de rede. O SWA lida com estes tipos de tráfego:

- Tráfego de dados: inclui o tráfego processado pelo Web Proxy de usuários finais que navegam na Internet.
- Tráfego de gerenciamento: abrange o tráfego gerado pelo gerenciamento do dispositivo através da interface da Web, bem como o tráfego para serviços de gerenciamento, como atualizações de SWA, atualizações de componentes, DNS, autenticação e outras tarefas relacionadas.

Por padrão, ambos os tipos de tráfego usam as rotas definidas para todas as interfaces de rede configuradas. No entanto, você tem a opção de separar o roteamento para que o tráfego de gerenciamento use uma tabela de roteamento de gerenciamento dedicada e o tráfego de dados use uma tabela de roteamento de dados separada.

Tráfego de gerenciamento	Tráfego de dados
IUweb SSH SNMP Autenticação, com controlador de domínio (configurável) Syslogs Envio por FTP DNS (configurável) Atualizar/Atualizar/Chave de recurso (configurável)	Proxy HTTP Proxy HTTPS Proxy FTP negociação de WCCP Solicitação ICAP com servidor DLP externo DNS (configurável) Atualizar/Atualizar/Chave de recurso (configurável) Autenticação com controlador de domínio (configurável)



Observação: se você selecionar a opção "Usar porta M1 somente para gerenciamento", uma tabela de roteamento adicional chamada de tabela de roteamento de dados será adicionada ao SWA. Essa tabela de roteamento tem apenas um gateway padrão configurável; todos os caminhos de roteamento adicionais devem ser configurados manualmente.

Informações Relacionadas

- [Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Guia de instalação do Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco](#)
- [Use as práticas recomendadas de dispositivos da Web seguros](#)
- [Configurar firewall para dispositivo seguro da Web](#)
- [Configurar certificado de descryptografia no aplicativo da Web seguro](#)

- [Configurar e solucionar problemas de SNMP em SWA](#)
- [Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server](#)
- [Habilitar canal/vídeo específico do YouTube e bloquear o restante do YouTube no SWA](#)
- [Entender o formato do registro de acesso HTTPS no Secure Web Appliance](#)
- [Acessar logs do dispositivo da Web seguro](#)
- [Ignorar autenticação no Secure Web Appliance](#)
- [Bloquear o tráfego no Secure Web Appliance](#)
- [Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.