Eerste configuratie van Secure Web applicatie configureren

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

SWA installeren

Eerste configuratie

- IP-adres configureren
- Standaardgateway configureren
- Traditionele licentie importeren
- DNS-server configureren
- Slimme licentie configureren
- Wizard Systeem instellen

Netwerkconfiguratie

Routing-tabel

Gerelateerde informatie

Inleiding

Dit document beschrijft de stappen die nodig zijn om de Secure Web Applicatie (SWA) voor het eerst te configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toediening van SWA.
- Fundamentele netwerkbeginselen.

Cisco raadt u aan het volgende te doen:

- Fysieke of virtuele SWA geïnstalleerd.
- Administratieve toegang tot de grafische gebruikersinterface van de SWA (GUI).
- Administratieve toegang tot de SWA Command Line Interface (CLI).
- Administratieve toegang tot de SWA-console.
- Geldige SWA-licentie of toegang tot Smart License Management-portal (voor het geval u

Smart License gebruikt).

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

SWA installeren

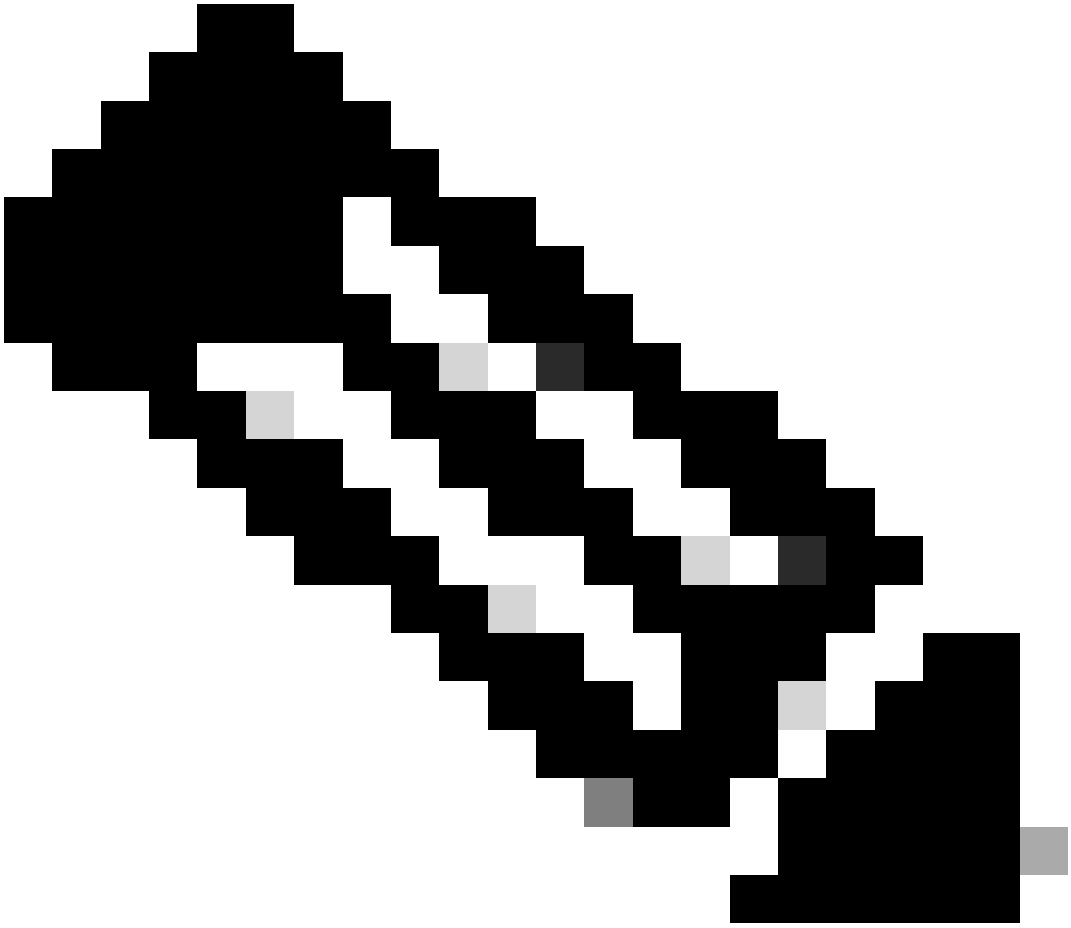
Cisco SWA is een proxyoplossing voor het voorwaartse segment die is ontworpen om de webbeveiliging en -controle voor organisaties te verbeteren. De SWA is zowel virtueel als fysiek beschikbaar en biedt flexibele implementatieopties om aan verschillende behoeften te voldoen. De virtuele SWA ondersteunt meerdere hypervisorplatforms, waaronder Microsoft Hyper-V, VMware ESX en KVM, en zorgt voor compatibiliteit met een groot aantal virtuele omgevingen. Voor gebruikers die de voorkeur geven aan een fysiek apparaat, biedt Cisco drie verschillende modellen aan: S100, S300 en S600. Elk model is ontworpen om te voldoen aan verschillende niveaus van prestaties en capaciteitsvereisten, waardoor organisaties de juiste pasvorm kunnen vinden voor hun specifieke webbeveiligingsbehoeften.

U kunt het image van uw virtuele machine downloaden op: https://software.cisco.com/download/home .

De virtuele Cisco SWA installeren is een eenvoudig proces dat begint met het selecteren van het juiste hypervisorplatform. Download eerst het installatiebestand van de virtuele SWA van de Cisco-website. Voor VMware ESX dient u het OVA-bestand te implementeren, zodat u de netwerkinstellingen kunt configureren en voldoende bronnen kunt toewijzen, zoals CPU, geheugen en opslag. Voor Microsoft Hyper-V moet u het gedownloade VHD-bestand importeren in de Hyper-V Manager en de instellingen van de virtuele machine dienovereenkomstig configureren. Gebruik voor KVM de virt-manager of de virsh opdrachtregel om de virtuele machine te definiëren en starten met behulp van het gedownloade image. Als de virtuele machine eenmaal in bedrijf is, kunt u de stappen in dit artikel gebruiken om de eerste configuratie uit te voeren.

Eerste configuratie

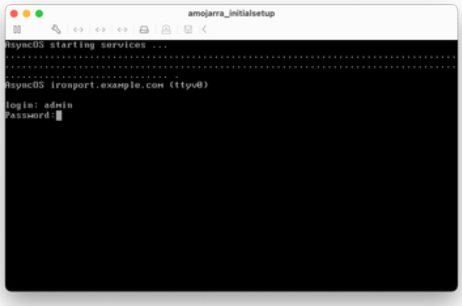
Nadat u de SWA hebt geïnstalleerd, gaat u verder met deze stappen voor een eerste implementatie.



Opmerking: voor de eerste configuratie moet u toegang tot SWA hebben via console, SSH en GUI.

Verbindingsmethode	Fase	Configuratiestappen
console	IP-adres configureren	Stap 1. Voer de gebruikersnaam en het wachtwoord in om in te loggen op de CLI.

Tip: De standaard gebruikersnaam is admin en het standaard wachtwoord is ironport.



Afbeelding - inlogscherm

Stap 2. Start ifconfig.

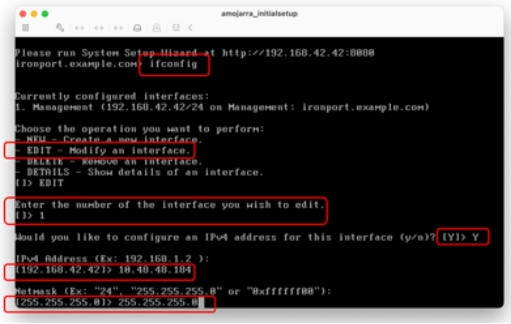
Stap 3. Kies Bewerken.

Stap 4. Voer het nummer in dat aan uw beheerinterface is gekoppeld.

Stap 5. Selecteer Y om het standaard IPv4-adres te bewerken.

Stap 6. Voer het IP-adres in

Stap 7. Voer het subnetmasker in.



Afbeelding - IP-adres voor beheerinterface bewerken

Stap 8. Als u IPv6 wilt configureren, typt u Y als antwoord op de vraag "Wilt u IPv6 configureren?". Anders kunt u dit als standaard laten staan (Nee) en drukt u op ENTER.

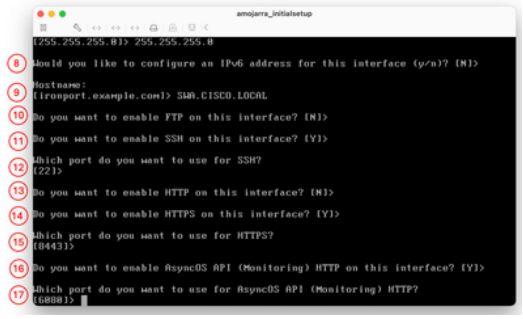
Stap 9. Voer een volledig gekwalificeerde domeinnaam (FQDN) in als de hostnaam.

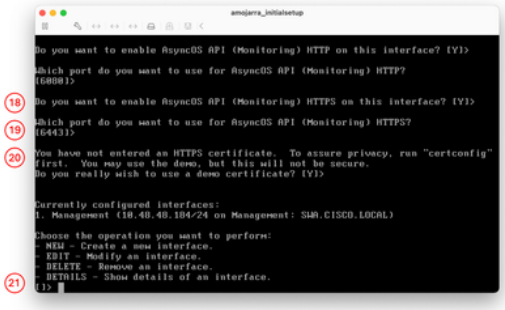
Stap 10. Als u de FTP-toegang (File Transfer Protocol) tot de beheerinterface wilt inschakelen, kiest u Y of drukt u op ENTER.

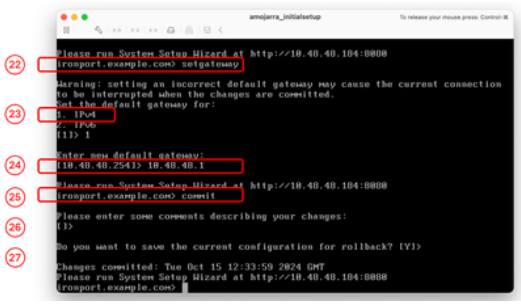
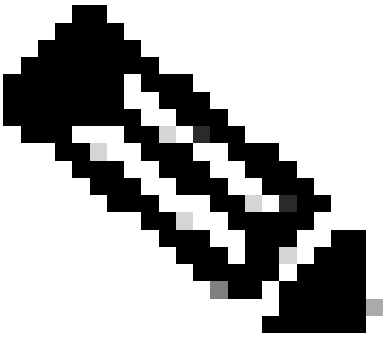
Stap 11. Secure Shell (SSH) is standaard ingesteld op Enabled. het is raadzaam om SSH ingeschakeld te hebben. Typ Y om door te gaan.

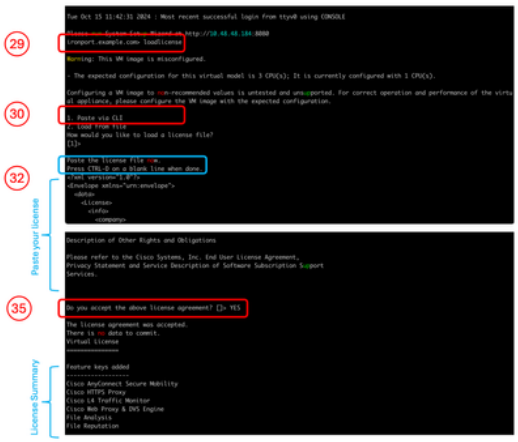
Stap 12. (optioneel) U kunt de standaard SSH poort van TCP 22 naar elk poortnummer wijzigen dat u wilt, zolang er geen poortconflicten zijn, druk op ENTER om de standaard poort te gebruiken (TCP/22).

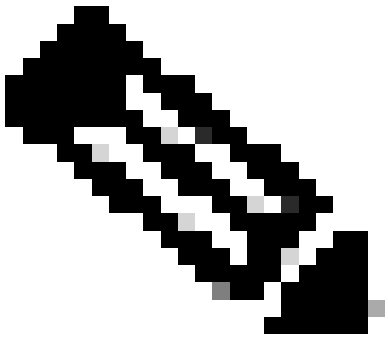
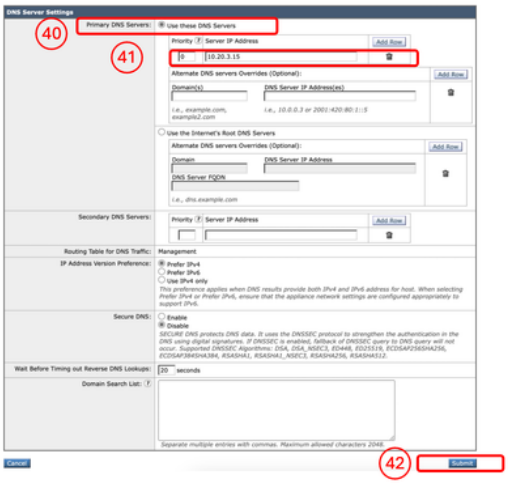
Stap 13. Als u HTTP-toegang (Hypertext Transfer Protocol) tot de beheerinterface wilt hebben, typt u Y en stelt u het poortnummer in voor HTTP-toegang. Anders kunt u ervoor kiezen N alleen toegang tot de beheerinterface te hebben via HTTPS (Hypertext Transfer Protocol

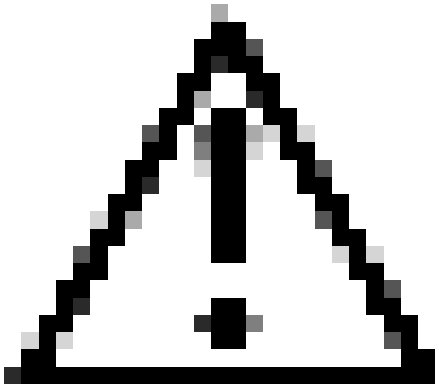
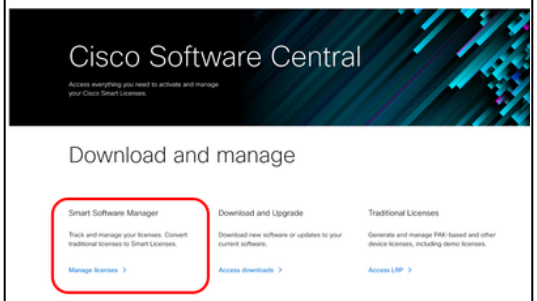
		Secure). Stap 14. Typ Y en druk op ENTER om HTTPS-toegang tot de beheerinterface mogelijk te maken. Stap 15. U kunt het standaard HTTPS poortnummer wijzigen van 8443 naar een poortnummer dat u wenst zolang er geen andere poortconflicten zijn, druk op ENTER om de standaardpoort te gebruiken (TCP/8443). Stap 16. Application Programming Interface (API) is standaard ingesteld op Enable, als u geen API gebruikt, kunt u de API uitschakelen door N te typen en op ENTER te drukken. Stap 17. Als u ervoor kiest om de API ingeschakeld te laten, kunt u het standaard API-poortnummer van 6080 wijzigen in een poortnummer dat u wenst, zolang er geen andere poortconflicten zijn, druk op ENTER om de standaardpoort te gebruiken (TCP/6080).  Image - Serviceconfiguratie voor beheerinterface Stap 18. AsyncOS API (monitoring) is de nieuwe GUI op de SWA. Als u de nieuwe gebruikersinterfacerapporten wilt gebruiken, stelt u deze optie in op Y (standaard), anders kunt u N typen en overslaan naar Stap 20

		Stap 19. U kunt het standaard nieuwe GUI HTTPS-poortnummer van 6443 naar elk poortnummer wijzigen dat u wenst zolang er geen andere poortconflicten zijn, druk op ENTER om de standaardpoort te gebruiken (TCP/6443). Stap 20. SWA Management Interface gebruikt Cisco-democertificaat. Type Y om het Demo-certificaat te accepteren. U kunt het GUI-certificaat wijzigen na de eerste configuratie. Stap 21. Druk op ENTER om de wizard ifconfig te verlaten.  Afbeelding - Nieuwe GUI TCP-configuratie
	Standaardgateway configureren	Stap 22. Start setgateway. Stap 23. Kies IPv4 als uw beheerinterface is geconfigureerd met IPv4, kies IPv6. Stap 24. Voer uw standaardgateway-IP-adres in. Stap 25. Sla de wijzigingen op door commit uit te voeren. Stap 26. (optioneel) U kunt opmerkingen toevoegen over de wijzigingen die u opslaat Stap 27. (optioneel) U kunt SWA hebben om een back-up te maken van de configuratie voordat u de

		wijzigingen toepast.  Afbeelding - De standaardgateway configureren
SSH	Traditionele licentie importeren	 Opmerking: als u Smart License gebruikt, gaat u naar Stap 36. Stap 28. Verbind met SWA via SSH. Stap 29. Licentie voor laden uitvoeren Stap 30. Kies Plakken via CLI. Stap 31. Open uw licentiebestand met een teksteditor en kopieer alle inhoud Stap 32. Plakt de licentie in de SSH-shell. Stap 33. Druk op ENTER om naar een nieuwe regel te navigeren. Stap 34. Houd Control ingedrukt en druk op D. Stap 35. Lees de

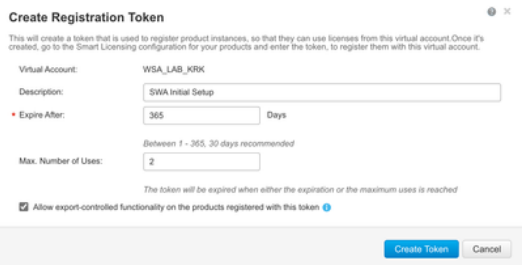
		Licentieovereenkomst en typ JA om akkoord te gaan met de voorwaarden.  Afbeelding - Traditionele licentie importeren Ga verder met Stap 58.
GUI	DNS-server configureren	Stap 37. Log in op de GUI (de standaardinstelling is HTTPS://<SWA FQDN of IP-adres>:843) Stap 38. Navigeer naar Netwerk en kies DNS. Stap 39. Klik op Instellingen bewerken. Stap 40. Selecteer in het gedeelte Primaire DNS-servers de optie Deze DNS-servers gebruiken. Stap 41. Stel de prioriteit in op 0 en voer het IP-adres van uw DNS-server in.

		 Opmerking: u kunt meer dan één DNS-server toevoegen door Rij toevoegen te kiezen. Stap 42. Indienen. Stap 43. Breng de wijzigingen aan.  Afbeelding - DNS-server configureren
	Slimme licentie configureren	Stap 44. Kies in de GUI van System Administration voor Smart Software Licensing. Stap 45. Kies Smart Software Licensing inschakelen.

		 Waarschuwing: u kunt niet terugdraaien van Smart License naar Classic License nadat u de Smart License-functie op uw apparaat hebt ingeschakeld. Stap 46. Klik op OK om de configuratie van de slimme licentie voort te zetten. Stap 47. Breng de wijzigingen aan. Stap 48. Meld u aan bij Cisco Software Central (https://software.cisco.com/#) om een token te verkrijgen voor het registreren van uw SWA Stap 49. Klik op Licenties beheren.  Afbeelding - Cisco Smart License Management Stap 50. Kies Inventaris in Smart Software Licensing. Stap 51. Maak in het tabblad Algemeen een nieuw token of gebruik uw beschikbare token.

Afbeelding - Inventarispagina voor slimme softwarelicenties

Stap 52. Voer de gewenste informatie in en maak een token.

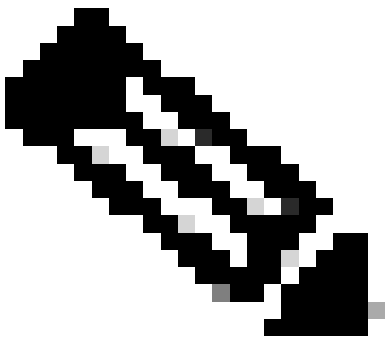


Afbeelding - Een token genereren

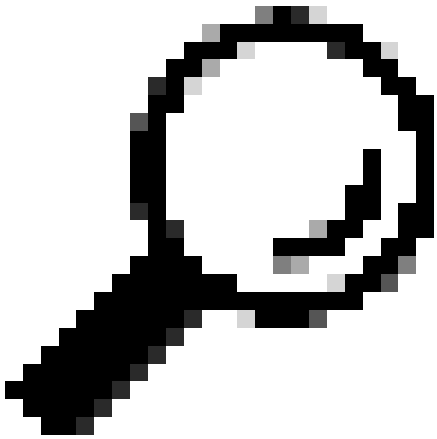
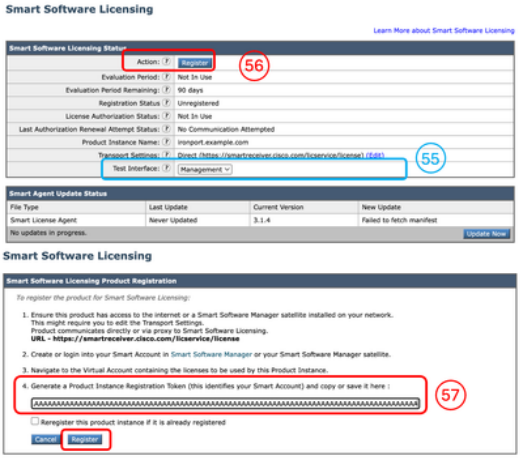
Stap 53. Klik op het blauwe pictogram voor het nieuwe token en kopieer de inhoud.

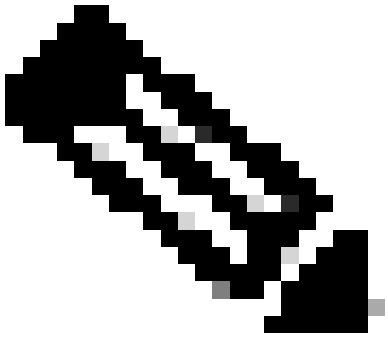
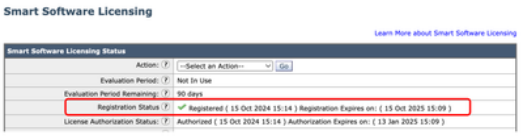
Afbeelding - De token kopiëren

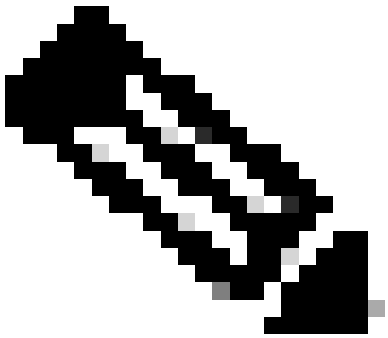
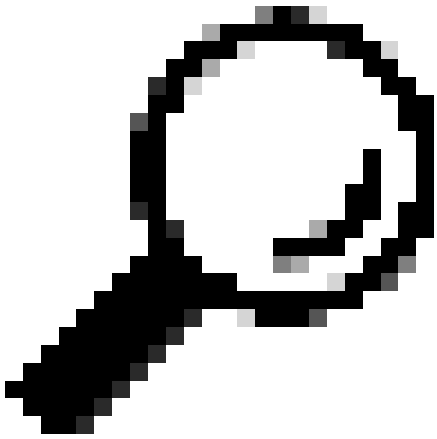
Stap 54. In de SWA GUI navigeer naar System Administration en kies Smart Software Licensing.



Opmerking: als u al op de pagina Smart Software

		Licensing staat, vernieuw dan de pagina. Stap 5. (optioneel) Als de SWA geen internettoegang heeft via de Management Interface, kunt u de Test Interface wijzigen in de Interfaces die toegang hebben tot internet.  Tip: Raadpleeg de sectie Netwerkconfiguratie in dit artikel voor meer informatie over meerdere interfaceconfiguraties en routingtabellen. Stap 56. Klik op Registreren. Stap 57. Plakt het token en klik op Registreren. 

		Afbeelding - Registreren SWA naar Smart License  Opmerking: om uw registratie te verifiëren, wacht u een paar minuten, vernieuw u de pagina Slimme licenties in SWA en controleer u de registratiestatus.  Afbeelding - Slimme licentiestatus
	Wizard Systeem instellen	Stap 58. In de SWA GUI navigeer naar System Administration en kies System Setup Wizard. Stap 59. De bepalingen van deze licentieovereenkomst lezen en aanvaarden Stap 60. Klik op Start Setup. Stap 61. Kiezen Standaard uit de Sectie Toestelmodus van werking. Stap 62. Voer de standaardnaam voor het systeem in.

		 Opmerking: vorige hostname die is gemaakt in Stap 9 was gerelateerd aan de Management Interface en niet de SWA. Stap 63. Voer het IP-adres van de DNS-server(s) in. Stap 64. u kunt uw Network Time Protocol (NTP)-server configureren.  Tip: Als uw NTP-server verificatie vereist, kunt u de sleutelparameters configureren. Stap 65. Selecteer de tijdzone die van toepassing is op de SWA en klik op Volgende.

Afbeelding - Wizard System Setup - Systeeminstellingen

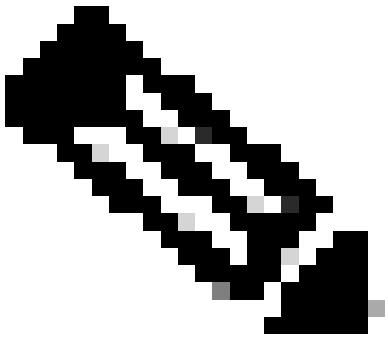
Stap 6. (optioneel) Als u een upstream proxy in uw netwerk gebruikt, kunt u deze configureren op de pagina Netwerkcontext of anders als standaard laten staan en op Volgende klikken.

Afbeelding - Wizard System Setup - Proxy-configuratie upstream

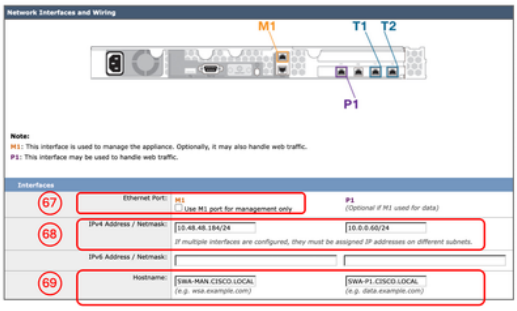
Stap 67. (optioneel) Selecteer Alleen de poort M1 voor beheer als u het verkeer van Management in-terface moet scheiden van het verkeer van Data Interfaces (P1- en P2-interfaces).

Stap 68. (optioneel) U kunt het IP-adres voor netwerkinterfaces toevoegen of wijzigen vanuit het gedeelte IPv4-adres/netmasker of IPv6-adres/netmasker.

Stap 69. (optioneel) U kunt de Hostname Network Interfaces toevoegen of wijzigen en op Volgende klikken.

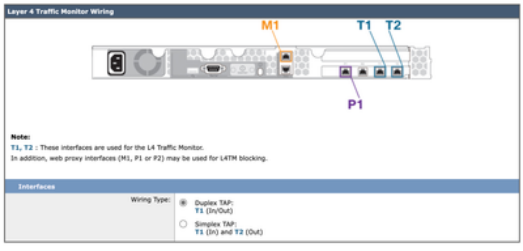


Opmerking: de P1-poort kan worden ingeschakeld en geconfigureerd via de Wizard System Setup. Als u de P2-interface wilt inschakelen, moet u dit doen nadat u de wizard System Setup (Systeeminstellingen) hebt voltooid.



Afbeelding - Wizard System Setup - Configuratie netwerkinterfaces

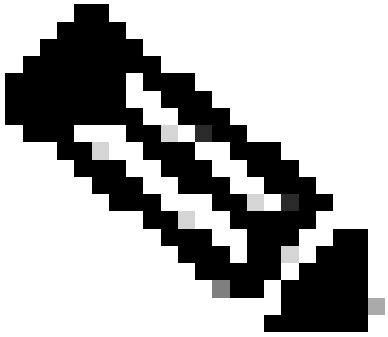
Stap 70. (optioneel) Als u Layer 4 Traffic Monitor (L4TM) wilt configureren, kunt u de duplexinstelling configureren, of anders kunt u als standaard vertrekken en op Volgende klikken.



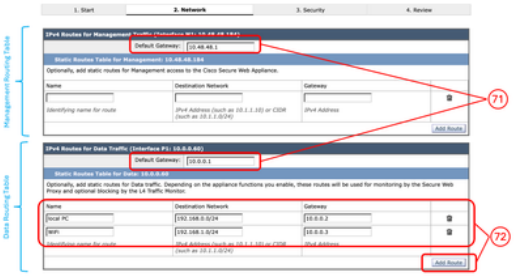
Afbeelding - Wizard System Setup - Layer 4 Traffic Monitor Settings

Stap 71. (optioneel) Op de pagina IPv4 Routes for Management kunt u de standaardgateway wijzigen

Stap 72. (optioneel) U kunt Route toevoegen om statische routes te maken.

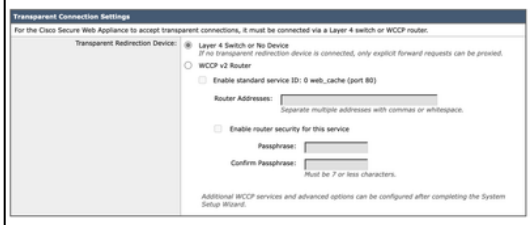
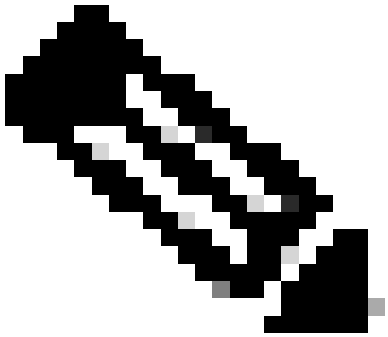


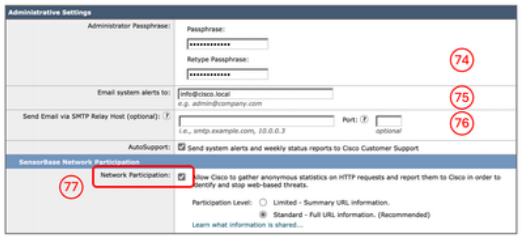
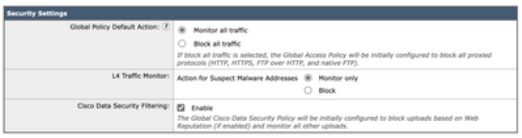
Opmerking: indien u "Alleen M1-poort voor beheer gebruiken" kiest in stap 67, dan zou er twee afzonderlijke Routing-tabel zijn voor de Management-interface en de Data-interfaces (P1 en P2).



Afbeelding - Wizard System Setup - Route toevoegen

Stap 73. (optioneel) Als u de implementatie van Transparent Proxy wilt instellen via Web Cache Communication Protocol (WCCP), kunt u WCCP-instellingen configureren of anders kunt u de

		standaard Layer 4-Switch of No Device verlaten en op Volgende klikken.  Image - System Setup Wizard - Proxy-implementatieconfiguratie Stap 74. Stel een nieuw wachtwoord in voor de admin-account. Stap 75. Voer een e-mailadres in dat naar verwachting systeemmeldingen zal ontvangen. Stap 76. (optioneel) Geef de hostinformatie van Simple Mail Transfer Protocol (SMTP) Relay, anders laat u deze leeg Als er geen interne relay host is gedefinieerd, gebruikt SMTP DNS lookup van de MX record. Stap 7. (optioneel) Als u deelname aan het Cisco SensorBase-netwerk wilt uitschakelen, deselecteert u het selectievakje Network Participation of laat u het veld standaard leeg en klikt u op Volgende.  Opmerking: deelname aan het Cisco SensorBase-

		netwerk betekent dat Cisco gegevens verzamelt en die informatie deelt met de SensorBase-bedreigingsbeheerdatabase.  Afbeelding - Wizard Systeem instellen - Instellingen voor beheer Stap 78. (optioneel) U kunt de standaardacties voor Global Policy, L4TM, en Cisco Data Security Filtering wijzigen, of u kunt deze als standaard laten staan en op Next klikken.  Afbeelding - Wizard System Setup - Beveiligingsinstellingen Stap 79. Bekijk uw configuratie. Als u wijzigingen moet aanbrengen, klikt u op de knop Vorige om terug te keren naar de vorige pagina of klikt u anders op Installeren.

Netwerkconfiguratie

Om de netwerkinterface te configureren kunt u zowel CLI als GUI gebruiken.

	Opdracht/pad	Actie
Netwerkinterfacekaarten configureren vanuit CLI	CLI >bestandsconfiguratie	Nieuw: Als de interface niet in de ifconfig-uitvoer wordt

		vermeld, maar in de virtuele machine of de fysieke applicatie bestaat, kunt u deze opdracht gebruiken om de interface in de lijst weer te geven. Bewerken: Deze actie is om het IP-adres, subnetmasker, interface-hostnaam of andere gerelateerde parameters te bewerken. Details: Toon details van een interface, zoals MAC-adres, mediatype, duplexmodus en ga zo maar door. Verwijderen: Verwijdert de interface uit de ifconfig lijst en verwijdert het IP adres indien eerder toegewezen.
Netwerkinterfacekaarten configureren vanuit GUI	GUI >Netwerk > interfaces	U kunt het IP-adres en de hostnaam van de interface bewerken. U kunt het poortnummer van de Toepassingsbeheerservices zoals FTP, SSH, HTTP-toegang en HTTPS-toegang.

Routing-tabel

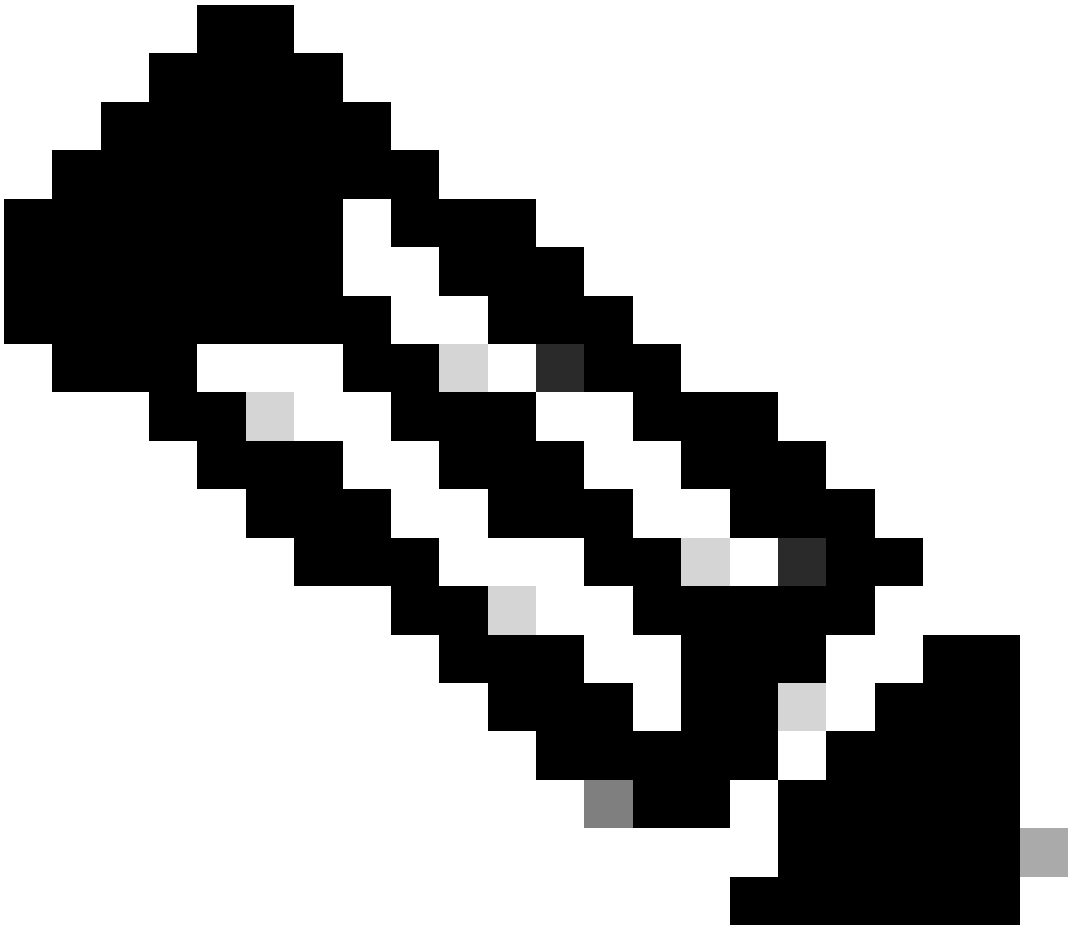
Routes zijn essentieel om te bepalen waar netwerkverkeer moet worden geleid. De SWA verwerkt dit soort verkeer:

- Gegevensverkeer: Dit omvat verkeer dat door de Web Proxy van eindgebruikers wordt verwerkt die Internet doorbladeren.
- Beheerverkeer: dit omvat verkeer dat wordt gegenereerd door het beheer van het apparaat via de webinterface, en verkeer voor beheerservices zoals SWA-upgrades, component-updates, DNS, verificatie en andere verwante taken.

In de standaardinstelling worden beide verkeerstypen gebruikt voor de routes die voor alle geconfigureerde netwerkinterfaces zijn gedefinieerd. U hebt echter de optie om de routing van

elkaar te scheiden, zodat het beheerverkeer gebruik maakt van een specifieke beheerrouteringstabel en het gegevensverkeer gebruik maakt van een afzonderlijke tabel voor het routing van gegevens.

Beheerverkeer	Gegevensverkeer
Webex UI SSH SNMP Verificatie, met domeincontroller (configureerbaar) Syslogs FTP-push DNS (configureerbaar) Update/upgrade/functiesleutel (configureerbaar)	HTTP-proxy HTTPS-proxy FTP-proxy WCCP-onderhandeling ICAP-verzoek met externe DLP-server DNS (configureerbaar) Update/upgrade/functiesleutel (configureerbaar) Verificatie met domeincontroller (configureerbaar)



Opmerking: als u de optie "Alleen M1-poort voor beheer gebruiken" selecteert, wordt een extra routeringstabel, de tabel Gegevensrouting, aan de SWA toegevoegd. Deze routeringstabel heeft slechts één configureerbare standaardgateway; alle extra routeringpaden moeten handmatig worden geconfigureerd.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web applicatie
- Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance
- Aangepaste URL-categorieën configureren in applicatie voor beveiligd web - Cisco
- Best practices voor beveiligde web applicatie gebruiken
- Firewall voor beveiligde web applicatie configureren
- Configureren van decryptie-certificaat in beveiligde web applicatie
- SNMP in SWA configureren en problemen oplossen
- SCP Push Logs in Secure Web Applicatie configureren met Microsoft Server
- Schakel specifieke YouTube Channel/Video en Blokkeer rest van YouTube in SWA
- HTTPS-toegangslogindeling begrijpen in Secure Web-applicatie
- Logbestanden van beveiligde web-applicatie openen
- Verificatie via bypass in beveiligde web-applicatie
- Blokverkeer in beveiligde web-applicatie
- Mis Microsoft Updates Traffic in Secure Web applicatie

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.