Configuration initiale de Secure Web Appliance

Table des matières

Introduction

Ce document décrit les étapes requises pour configurer l'appareil Web sécurisé (SWA) pour la première fois.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.
- Principes fondamentaux des réseaux.

Cisco recommande que vous ayez :

- SWA physique ou virtuel installé.
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA.
- Accès administratif à l'interface de ligne de commande (CLI) SWA.
- Accès administratif à la console SWA.
- Licence SWA valide ou accès au portail Smart License Management (si vous utilisez la licence Smart).

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Installation de SWA

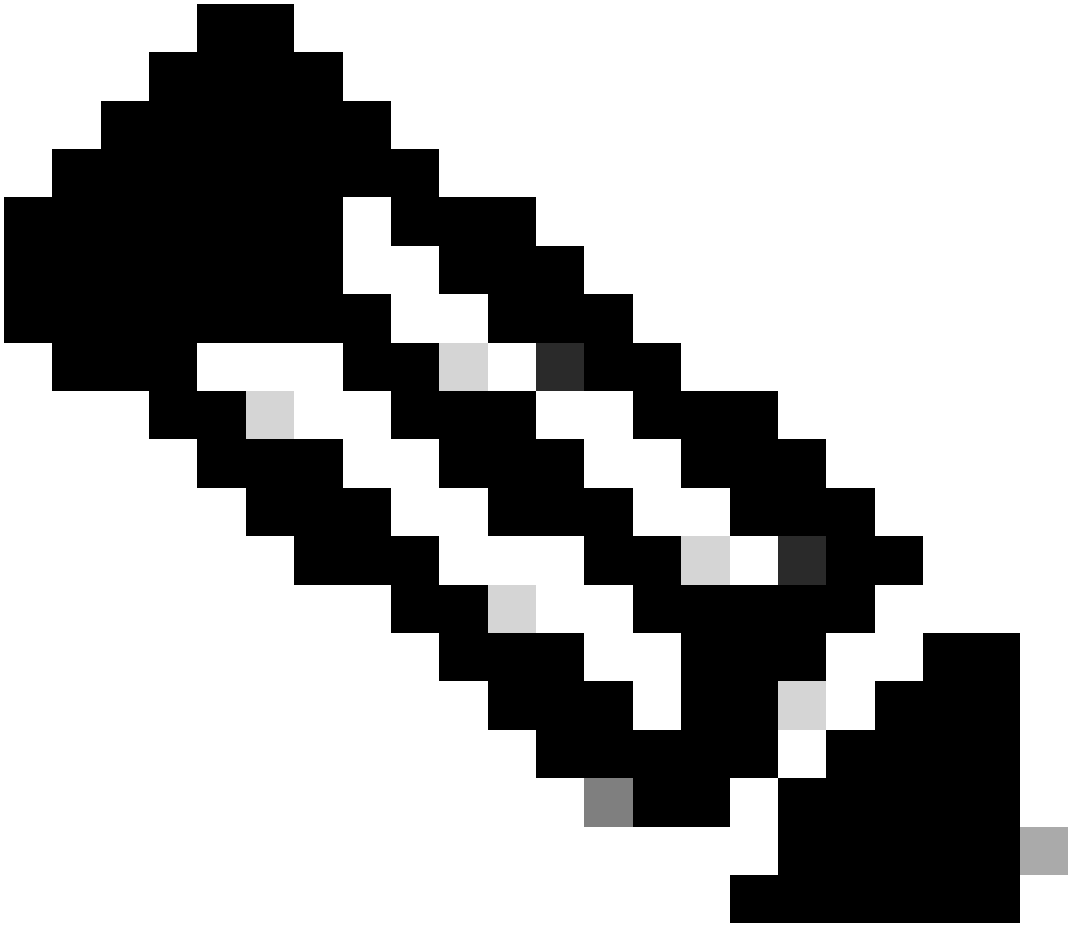
Cisco SWA est une solution de proxy avant conçue pour améliorer la sécurité et le contrôle du web pour les entreprises. Disponible sous forme virtuelle et physique, le SWA offre des options de déploiement flexibles pour répondre à divers besoins. Le SWA virtuel prend en charge plusieurs plates-formes d'hyperviseur, notamment Microsoft Hyper-V, VMware ESX et KVM, assurant ainsi la compatibilité avec une gamme d'environnements virtuels. Pour ceux qui préfèrent une appliance physique, Cisco propose trois modèles distincts : S100, S300 et S600. Chaque modèle est conçu pour répondre à différents niveaux de performances et d'exigences de capacité, afin de garantir que les entreprises peuvent trouver la solution adaptée à leurs besoins spécifiques en matière de sécurité Web.

Pour télécharger l'image de votre machine virtuelle, rendez-vous à l'adresse suivante : https://software.cisco.com/download/home .

L'installation de Cisco SWA virtuel est un processus simple qui commence par la sélection de la plate-forme d'hyperviseur appropriée. Tout d'abord, téléchargez le fichier d'installation virtuelle de SWA depuis le site Web de Cisco. Pour VMware ESX, déployez le fichier OVA, en vous assurant de configurer les paramètres réseau et d'allouer suffisamment de ressources telles que le processeur, la mémoire et le stockage. Pour Microsoft Hyper-V, importez le fichier VHD téléchargé dans le Gestionnaire Hyper-V et configurez les paramètres de l'ordinateur virtuel en conséquence. Pour KVM, utilisez l'outil en ligne de commande virt-manager ou virsh pour définir et démarrer la machine virtuelle à l'aide de l'image téléchargée. Une fois que la machine virtuelle est opérationnelle, vous pouvez utiliser les étapes de cet article pour effectuer la configuration initiale.

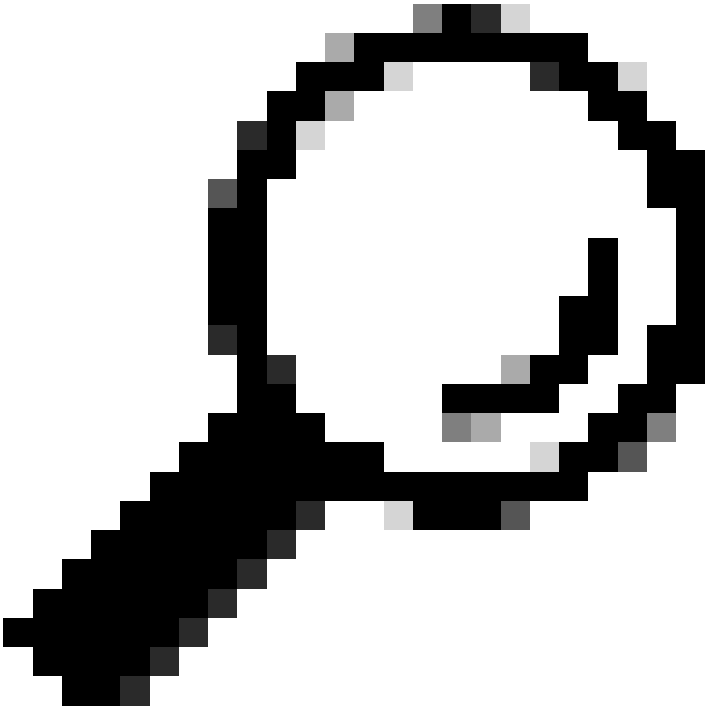
Configuration initiale

Après avoir installé le SWA, procédez comme suit pour le déploiement initial.



Remarque : pour la configuration initiale, vous devez avoir accès à SWA via la console, SSH et GUI.

Méthode de connexion	Étape	Configuration Steps
Console	Configurer l'adresse IP	Étape 1. Saisissez le nom d'utilisateur et le mot de passe pour vous connecter à la CLI.



Conseil : le nom d'utilisateur par défaut est admin et le mot de passe par défaut est ironport.

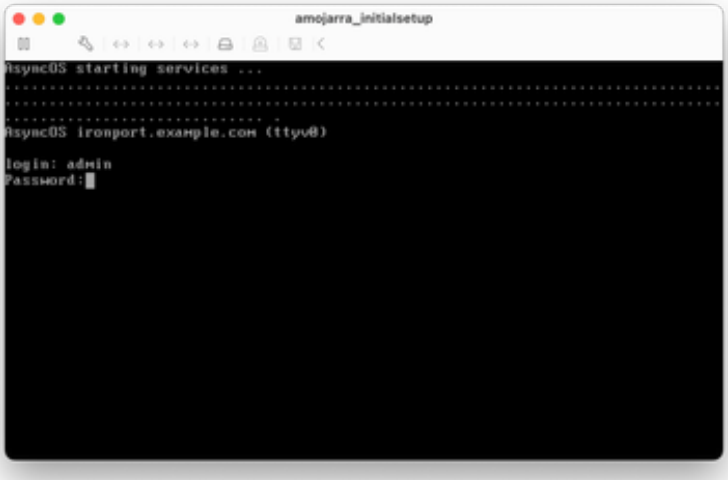


Image - écran de connexion

Étape 2. Exécutez ifconfig.

Étape 3. Sélectionnez Modifier.

Étape 4. Saisissez le numéro associé à votre interface de gestion.

Étape 5. Sélectionnez Y pour modifier l'adresse IPv4 par défaut.

Étape 6. Saisissez l'adresse IP

Étape 7. Saisissez le masque de sous-réseau.

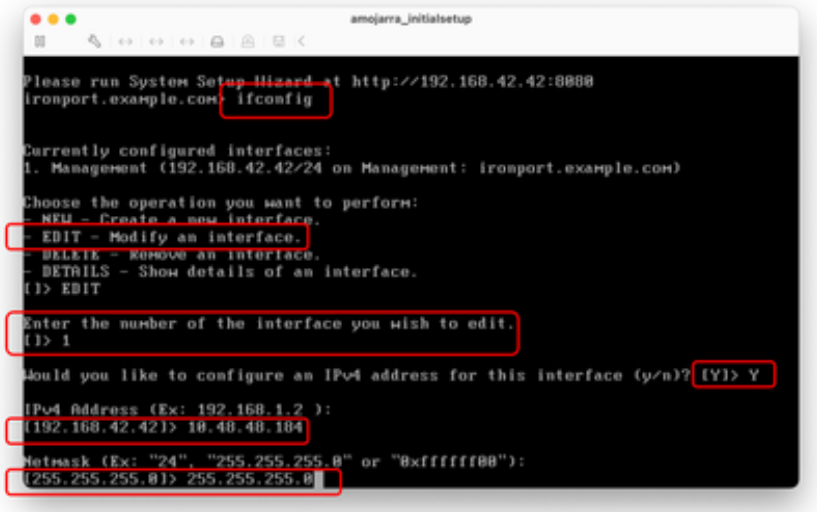


Image - Modifier l'adresse IP de l'interface de gestion

Étape 8. Si vous souhaitez configurer IPv6, tapez Y en réponse à la question « Voulez-vous configurer IPv6 ? », sinon vous pouvez laisser cette valeur par défaut (Non) et appuyer sur Entrée.

Étape 9. Entrez un nom de domaine complet (FQDN) comme nom d'hôte.

Étape 10. Si vous souhaitez activer l'accès FTP (File Transfer Protocol) à l'interface de gestion, sélectionnez Y, ou appuyez sur Entrée.

Étape 11. Par défaut, Secure Shell (SSH) est défini sur Enabled (Activé). Il est conseillé d'activer SSH. Tapez Y pour continuer.

Étape 12. (Facultatif) Vous pouvez remplacer le port SSH par défaut TCP/22 par n'importe quel numéro de port que vous souhaitez, tant qu'il n'y a pas de conflit de port, appuyez sur Entrée pour utiliser le port par défaut (TCP/22).

Étape 13. Si vous souhaitez disposer d'un accès HTTP (Hypertext Transfer Protocol) à l'interface de gestion, tapez Y et définissez le numéro de port pour l'accès HTTP. Sinon, vous pouvez choisir N pour avoir uniquement un accès HTTPS (Hypertext Transfer Protocol Secure) à l'interface de gestion.

Étape 14. Tapez Y et appuyez sur Entrée pour activer l'accès HTTPS à l'interface de gestion.

Étape 15. Vous pouvez remplacer le numéro de port HTTPS par défaut 8443 par n'importe quel numéro de port souhaité, tant qu'il n'y a pas de conflit de port, appuyez sur Entrée pour utiliser le port par défaut (TCP/8443).

Étape 16. L'interface de programmation d'application (API) par défaut est définie sur Activer, si vous n'utilisez pas l'API, vous pouvez désactiver l'API en tapant N et en appuyant sur Entrée.

Étape 17. Si vous choisissez d'activer l'API, vous pouvez remplacer le numéro de port par défaut de l'API 6080 par n'importe quel numéro de port souhaité, tant qu'il n'y a pas de conflit de port, appuyez sur Entrée pour utiliser le port par défaut (TCP/6080).

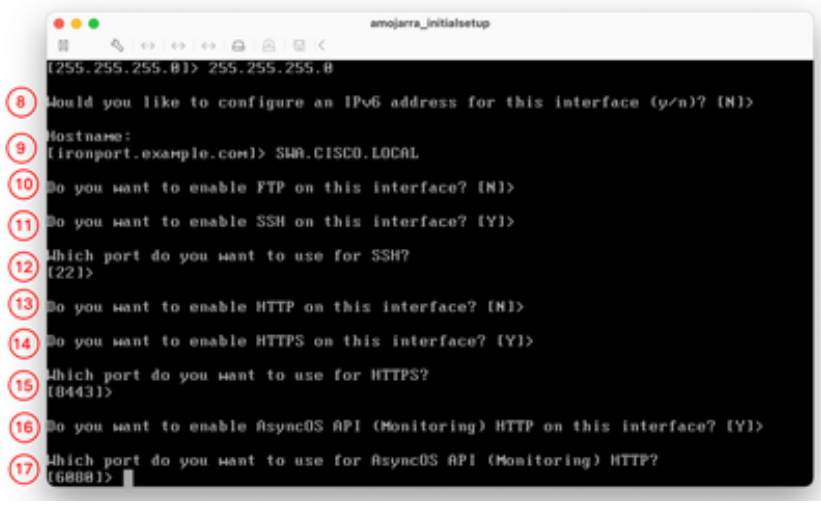
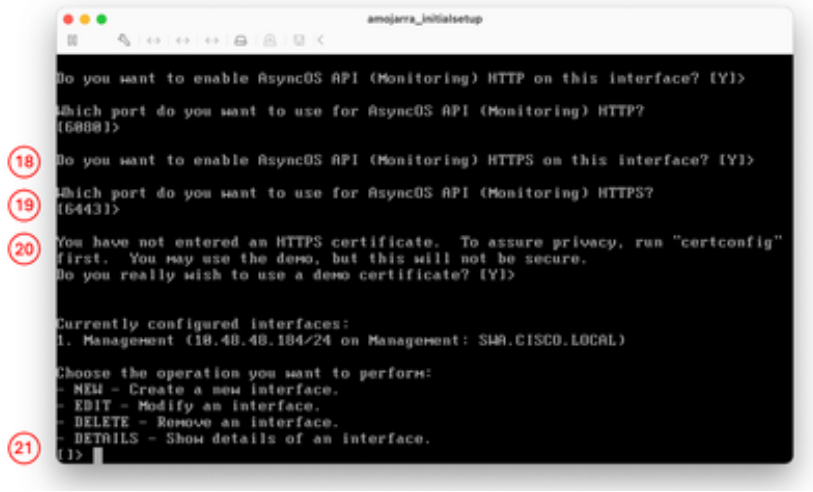


Image - Configuration du service d'interface de gestion

Étape 18. L'API AsyncOS (surveillance) est la nouvelle interface graphique utilisateur du SWA. Si vous souhaitez utiliser les nouveaux rapports d'interface utilisateur, définissez cette option sur Y (par défaut). Sinon, vous pouvez taper N et passer à l'étape 20

Étape 19. Vous pouvez remplacer le numéro de port HTTPS par défaut de la nouvelle interface utilisateur graphique 6443 par n'importe quel numéro de port souhaité, tant qu'il n'y a pas de conflit de port, appuyez sur Entrée pour utiliser le port par défaut (TCP/6443).

Étape 20. L'interface de gestion SWA utilise le certificat de démonstration Cisco. Entrez Y pour accepter le certificat

		de démonstration. Vous pouvez modifier le certificat de l'interface utilisateur graphique après la configuration initiale. Étape 21. Appuyez sur Entrée pour quitter l'assistant ifconfig.  Image - Nouvelle configuration TCP de l'interface graphique
	Configurer la passerelle par défaut	Étape 22. Exécutez setgateway. Étape 23. Choisissez IPv4 si votre interface de gestion a été configurée avec IPv4, sinon choisissez IPv6. Étape 24. Entrez votre adresse IP de passerelle par défaut. Étape 25. Enregistrez les modifications en exécutant la commande commit. Étape 26. (Facultatif) vous pouvez ajouter des remarques sur les modifications que vous enregistrez Étape 27. (Facultatif) SWA peut sauvegarder la configuration avant d'appliquer les modifications.

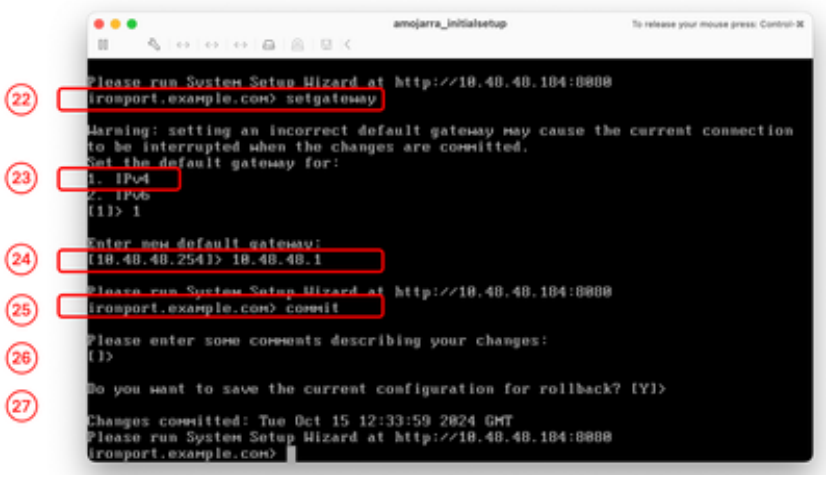
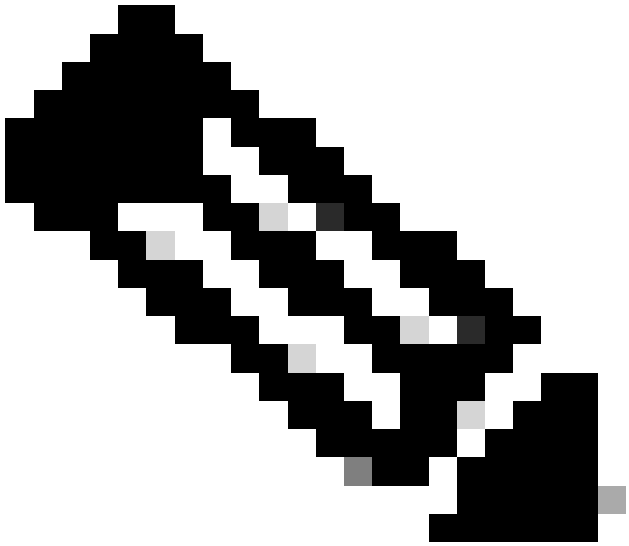
<table>
<tr>
<td></td>
<td></td>
<td> 

Image : configuration de la passerelle par défaut</td>
</tr>
<tr>
<td>SSH</td>
<td>Importer une licence traditionnelle</td>
<td> 
Remarque : si vous utilisez la licence Smart, passez à l'étape 36.

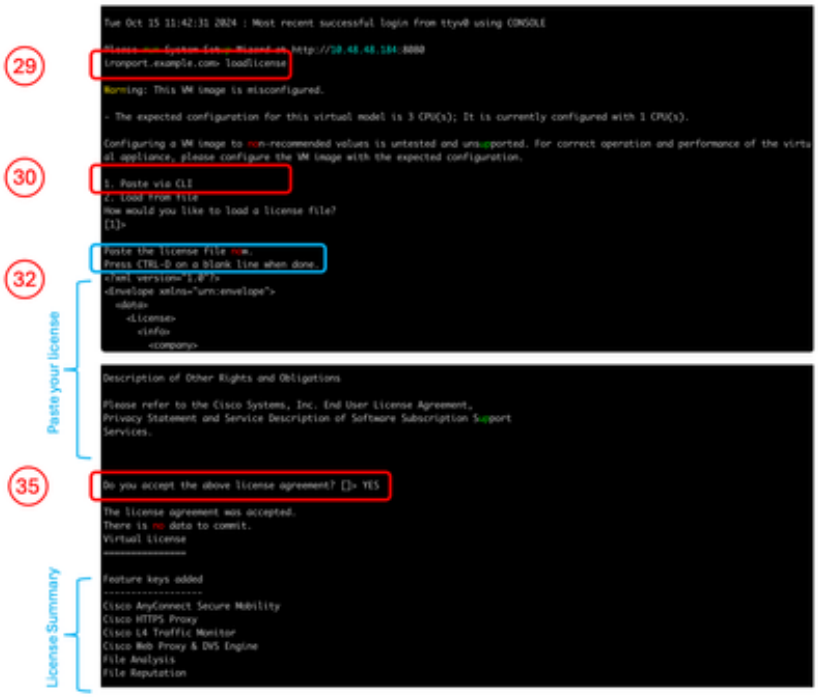
Étape 28. Connectez-vous à SWA via SSH.

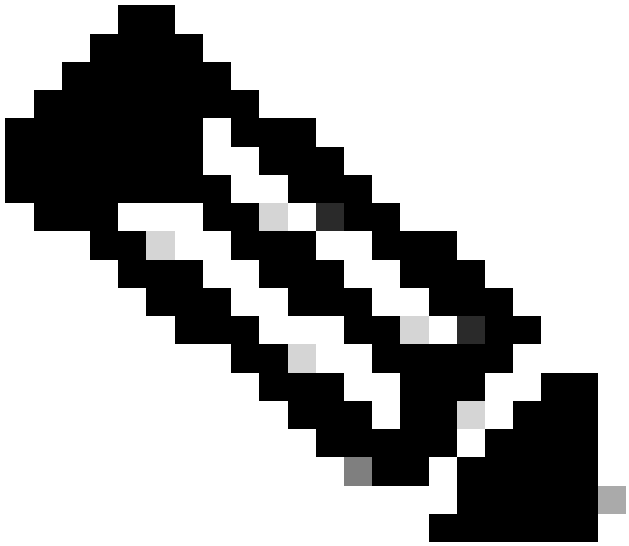
Étape 29. Exécuter loadlicense

Étape 30. Choisissez Paste via CLI.

Étape 31. Ouvrez votre fichier de licence avec un éditeur de texte et copiez tout son contenu

Étape 32. Collez la licence dans l'interpréteur de commandes SSH.</td>
</tr>
</table>

		Étape 33. Appuyez sur Entrée pour accéder à une nouvelle ligne. Étape 34. Maintenez la touche Ctrl enfoncée et appuyez sur D. Étape 35. Lisez le contrat de licence et tapez YES pour accepter les conditions.  Image - Importer une licence traditionnelle Passez à l'étape 58.
IUG	Configurer le serveur DNS	Étape 37. Connectez-vous à l'interface utilisateur graphique (HTTPS://<SWA FQDN or IP Address>:8443 par défaut) Étape 38. Accédez à Network et choisissez DNS. Étape 39. Cliquez sur Modifier les paramètres. Étape 40. dans la section Primary DNS Servers, sélectionnez Use these DNS Servers. Étape 41. Définissez la priorité sur 0 et entrez l'adresse IP de votre serveur DNS.



Remarque : vous pouvez ajouter plusieurs serveurs DNS en sélectionnant Ajouter une ligne.

Étape 42. Envoyer.

Étape 43. Validez les modifications.

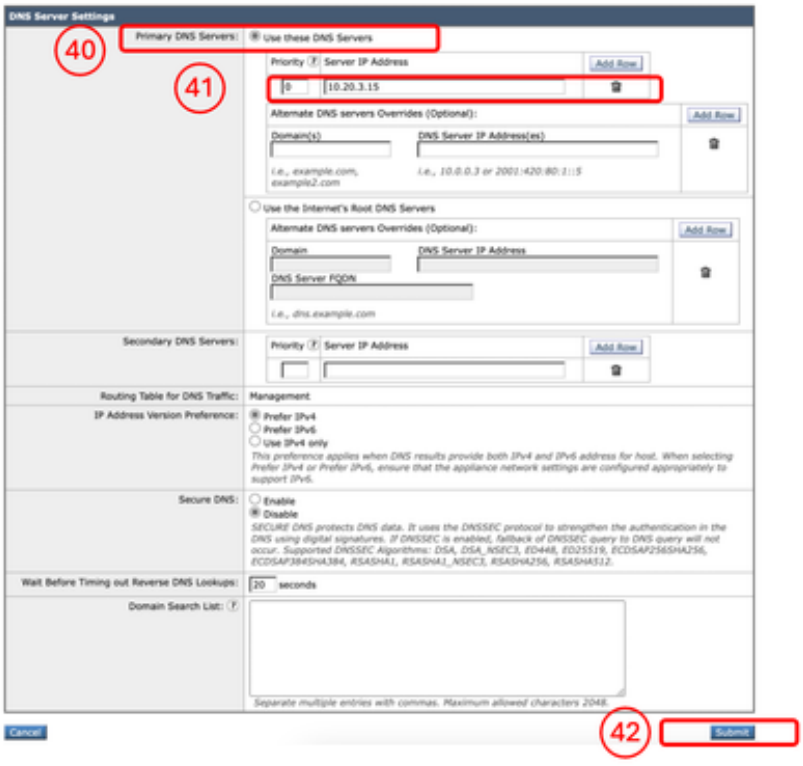
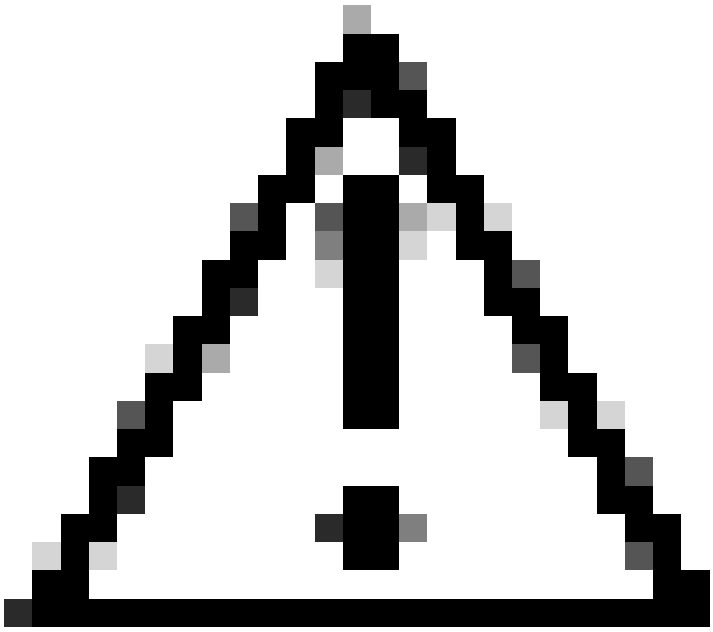


Image : configuration du serveur DNS

	Configurer la licence Smart	Étape 44. Dans l'interface utilisateur graphique de Administration système, sélectionnez Smart Software Licensing. Étape 45. Sélectionnez ActiverLicence logicielle Smart.  Attention : vous ne pouvez pas revenir de la licence Smart à la licence classique après avoir activé la fonction de licence Smart sur votre appliance. Étape 46. Cliquez sur OK pour poursuivre la configuration de la licence Smart. Étape 47. Validez les modifications. Étape 48. Pour obtenir le jeton permettant d'enregistrer votre SWA, connectez-vous à Cisco Software Central (https://software.cisco.com/#) Étape 49. Cliquez sur Gérer les licences.

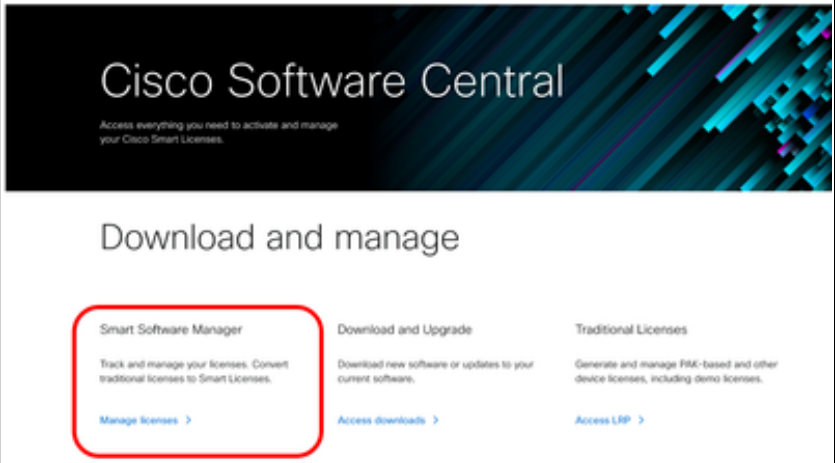


Image - Cisco Smart License Management

Étape 50. Dans Smart Software Licensing, sélectionnez Inventory.

Étape 51. Dans l'onglet General, créez un nouveau jeton ou utilisez vos jetons disponibles.

Image - Page Smart Software License Inventory

Étape 52. Entrez les informations requises et Create Token.

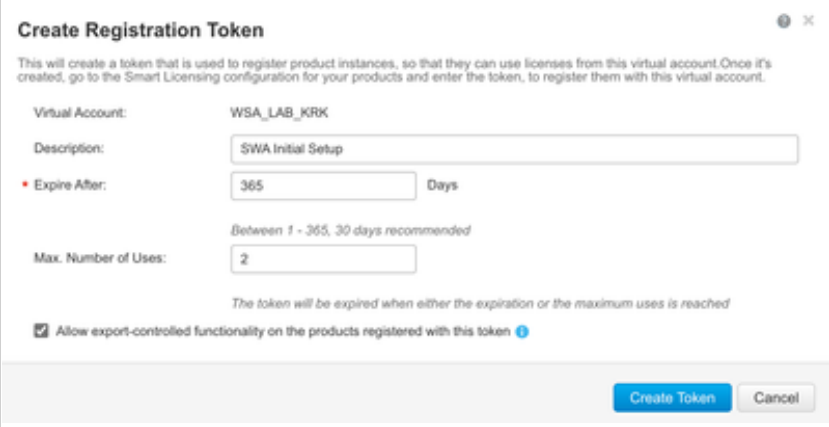


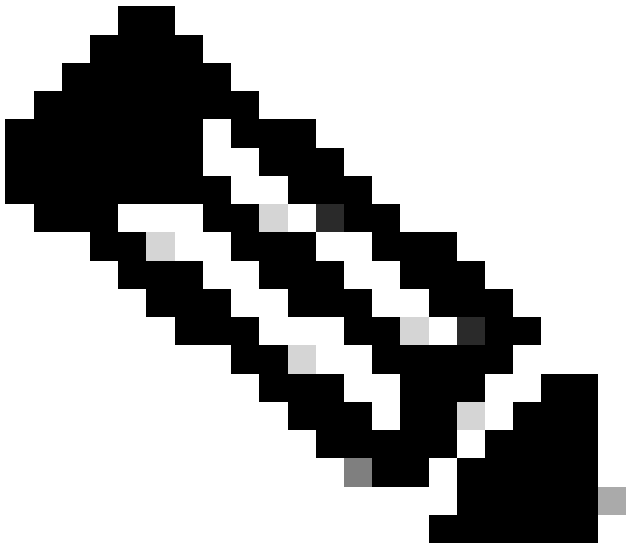
Image - Génération d'un jeton

Étape 53. Cliquez sur l'icône bleue en regard du nouveau

jeton et copiez son contenu.

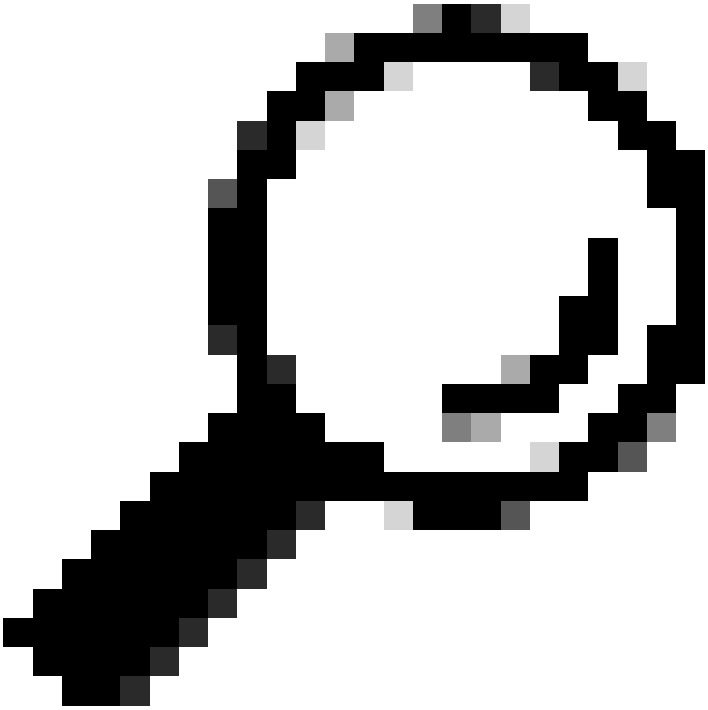
Image - Copier le jeton

Étape 54. Dans l'interface utilisateur graphique de SWA, accédez à Administration système et choisissez Smart Software Licensing.



Remarque : si vous êtes déjà sur la page Smart Software Licensing, actualisez-la.

Étape 55. (Facultatif) Si le SWA n'a pas d'accès à Internet depuis l'interface de gestion, vous pouvez remplacer l'interface de test par les interfaces autorisées à accéder à Internet.



Conseil : pour plus d'informations sur la configuration de plusieurs interfaces et les tables de routage, consultez la section Configuration réseau de cet article.

Étape 56. Cliquez sur Register.

Étape 57. Collez le jeton et cliquez sur Register.

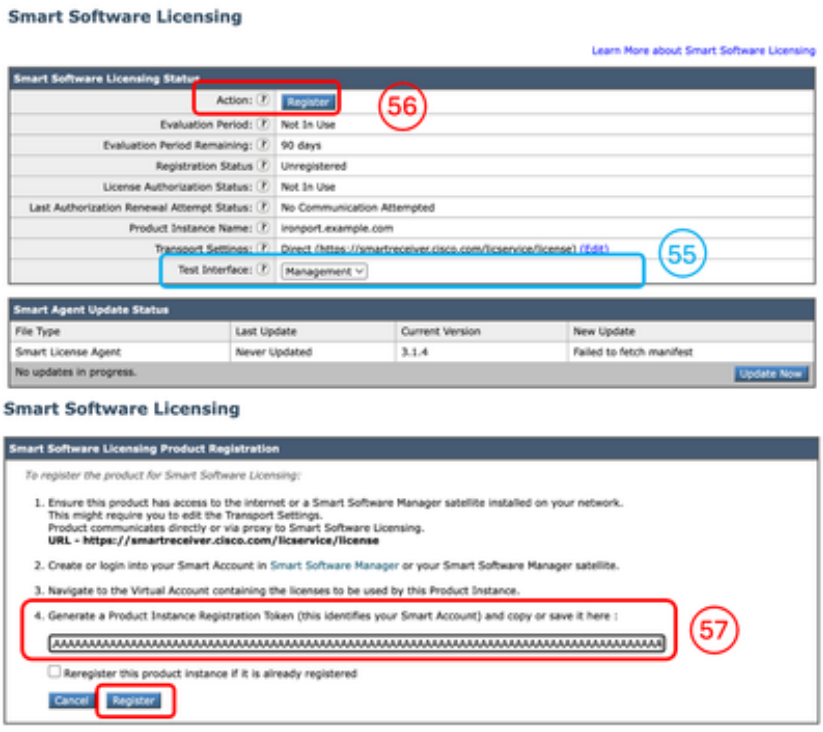
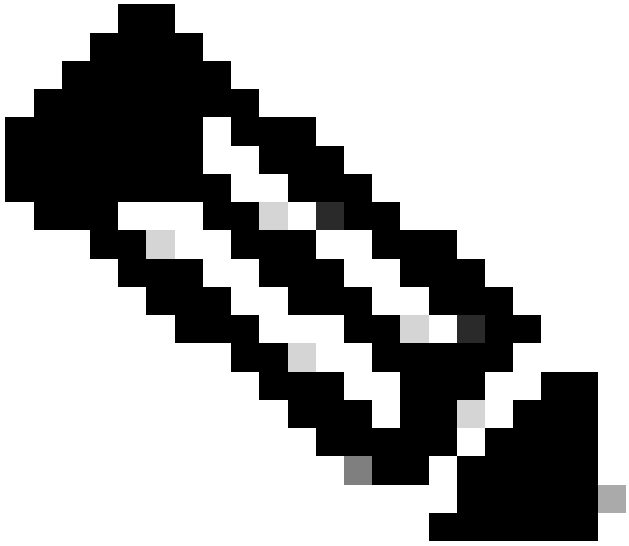
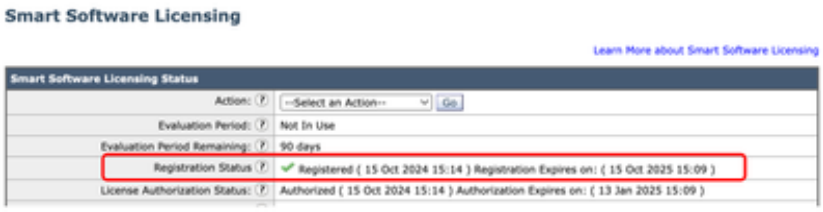
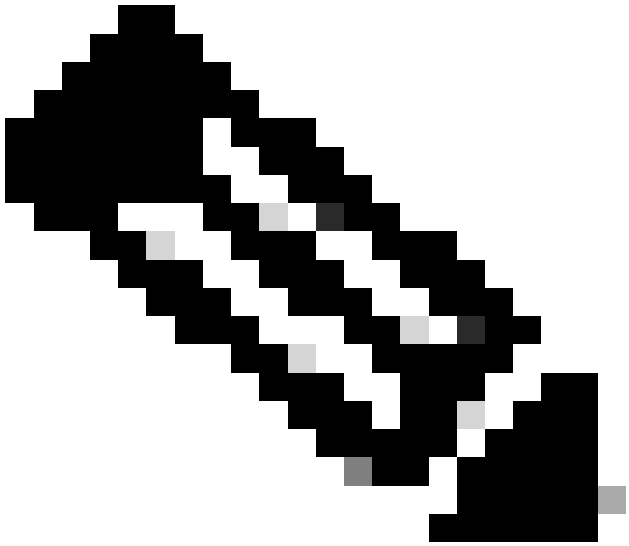
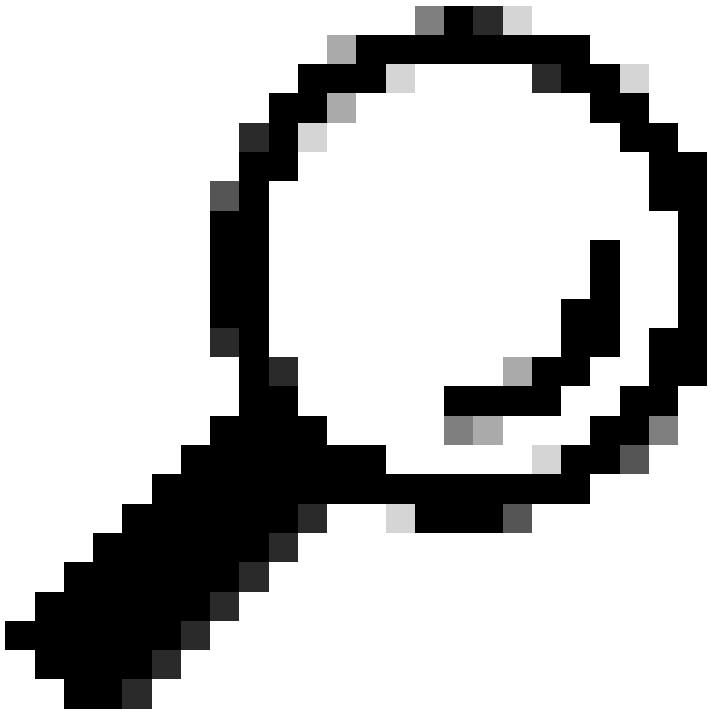


		Image - Enregistrer SWA sur la licence Smart  Remarque : pour vérifier votre inscription, attendez quelques minutes, actualisez la page Smart Licensing dans SWA et vérifiez l'état de l'inscription.  Image - État d'enregistrement des licences Smart
	Assistant de configuration du système	Étape 58. Dans l'interface utilisateur graphique de SWA, accédez à Administration système et choisissez Assistant de configuration du système. Étape 59. Lisez et acceptez les termes de ce contrat de licence Étape 60. Cliquez sur Commencer la configuration. Étape 61. Choisir Standard de la section Mode de fonctionnement de l'appareil. Étape 62. Saisissez le nom d'hôte système par défaut.

		 Remarque : le nom d'hôte précédent créé à l'étape 9 était lié à l'interface de gestion et non au SWA.
		Étape 63. Saisissez l'adresse IP du ou des serveurs DNS. Étape 64. Vous pouvez configurer votre serveur NTP (Network Time Protocol).
		 Conseil : si votre serveur NTP nécessite une

authentification, vous pouvez configurer les paramètres Key (Clé).

Étape 65. Sélectionnez le fuseau horaire qui s'applique au SWA et cliquez sur Next.

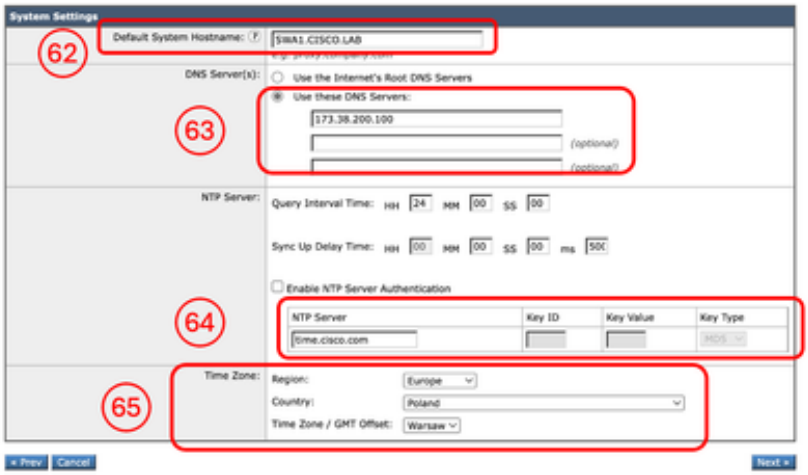


Image - Assistant de configuration du système - Paramètres système

Étape 66. (Facultatif) Si vous utilisez un proxy en amont dans votre réseau, vous pouvez le configurer sur la page Contexte réseau ou le laisser par défaut et cliquer sur Suivant.

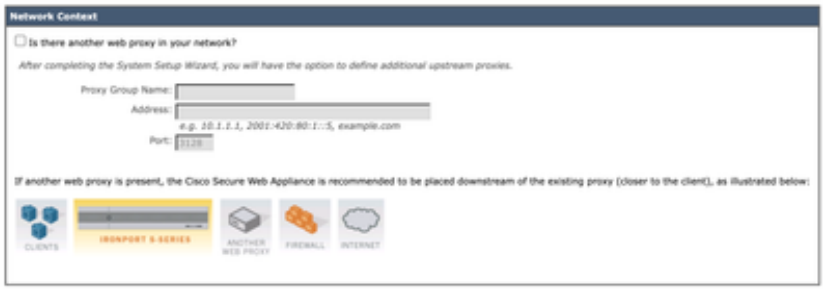


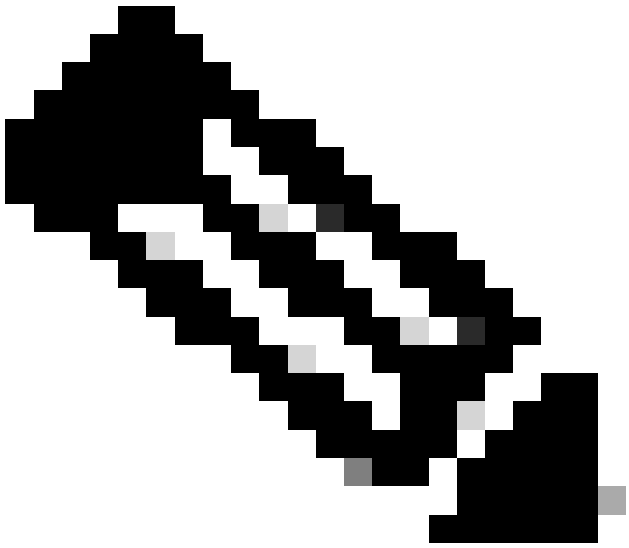
Image - Assistant de configuration du système - Configuration du proxy en amont

Étape 67. (Facultatif) Si vous devez séparer le trafic d'interface de gestion du trafic d'interfaces de données (interfaces P1 et P2), sélectionnez Utiliser le port M1 pour la gestion uniquement.

Étape 68. (Facultatif) Vous pouvez ajouter ou modifier l'adresse IP des interfaces réseau à partir de la section Adresse IPv4 / Masque réseau ou Adresse IPv6 / Masque réseau.

Étape 69. (Facultatif) Vous pouvez ajouter ou modifier le

nom d'hôte des interfaces réseau et cliquer sur Suivant.



Remarque : le port P1 peut être activé et configuré via l'Assistant de configuration du système. Si vous souhaitez activer l'interface P2, vous devez le faire après avoir terminé l'Assistant de configuration du système.

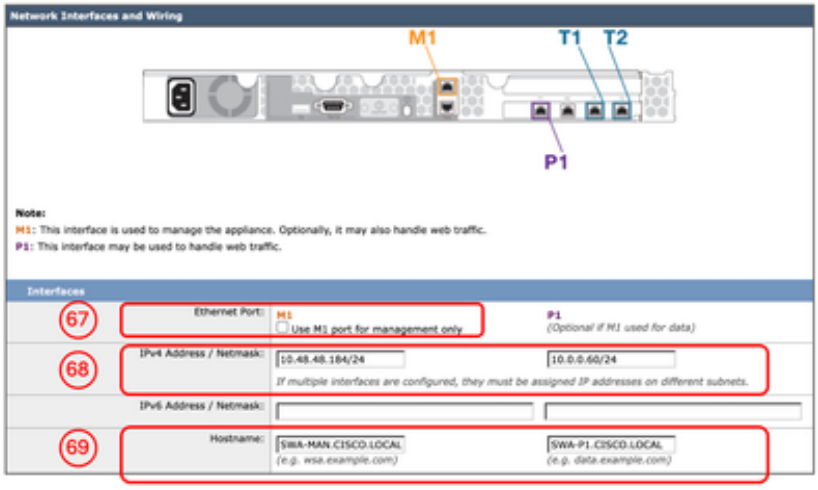


Image - Assistant de configuration du système - Configuration des interfaces réseau

Étape 70. (Facultatif) Si vous envisagez de configurer le Moniteur de trafic de couche 4 (L4TM), vous pouvez configurer le paramètre Duplex, ou vous pouvez laisser par défaut et cliquer sur Suivant.

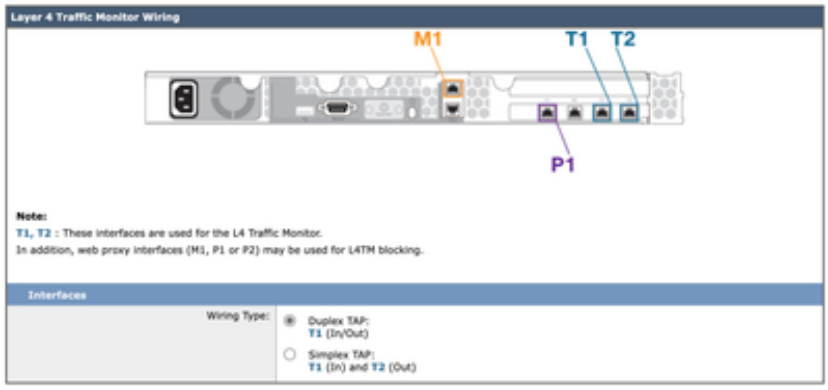
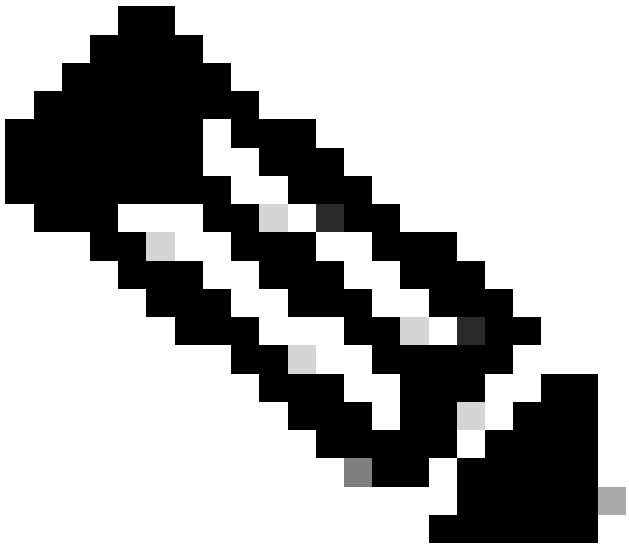


Image - Assistant de configuration du système - Paramètres du Moniteur de trafic de couche 4

Étape 71. (Facultatif) Dans la page Routes IPv4 pour la gestion, vous pouvez modifier la passerelle par défaut

Étape 72. (Facultatif) Vous pouvez ajouter une route pour créer des routes statiques.



Remarque : si vous choisissez « Utiliser le port M1 pour la gestion uniquement » à l'étape 67, il y aura deux tables de routage distinctes pour l'interface de gestion et les interfaces de données (P1 et P2).

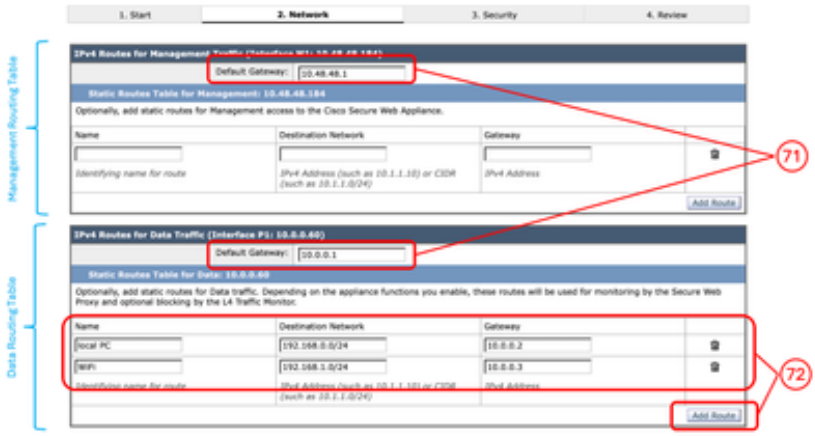


Image - Assistant de configuration du système - Ajouter un routage

Étape 73. (Facultatif) Si vous souhaitez configurer le déploiement du proxy transparent, via le protocole WCCP (Web Cache Communication Protocol), vous pouvez configurer les paramètres WCCP, ou vous pouvez laisser le commutateur de couche 4 par défaut ou Aucun périphérique et cliquer sur Suivant.

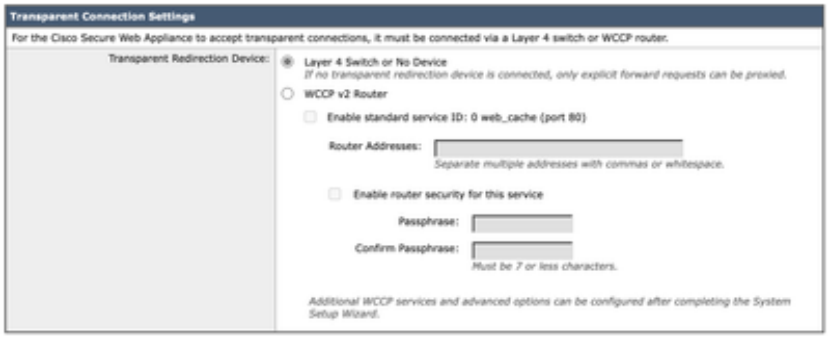


Image - Assistant Configuration du système - Configuration du déploiement du proxy

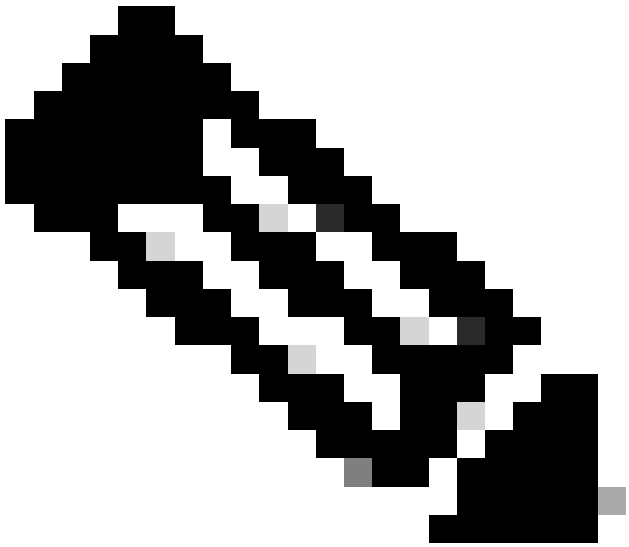
Étape 74. Configurez un nouveau mot de passe pour le compte admin.

Étape 75. Saisissez l'adresse e-mail qui doit recevoir les alertes système.

Étape 76. (Facultatif) Fournissez les informations sur l'hôte du relais SMTP (Simple Mail Transfer Protocol), sinon laissez-les vides Si aucun hôte de relais interne n'est défini, SMTP utilise la recherche DNS de l'enregistrement MX.

Étape 77. (Facultatif) Si vous souhaitez désactiver Participating in the Cisco SensorBase Network, désactivez la case à cocher Network Participation, ou

sinon laissez is comme valeur par défaut et cliquez sur Next.



Remarque : la participation au réseau Cisco SensorBase signifie que Cisco collecte des données et les partage avec la base de données de gestion des menaces SensorBase.

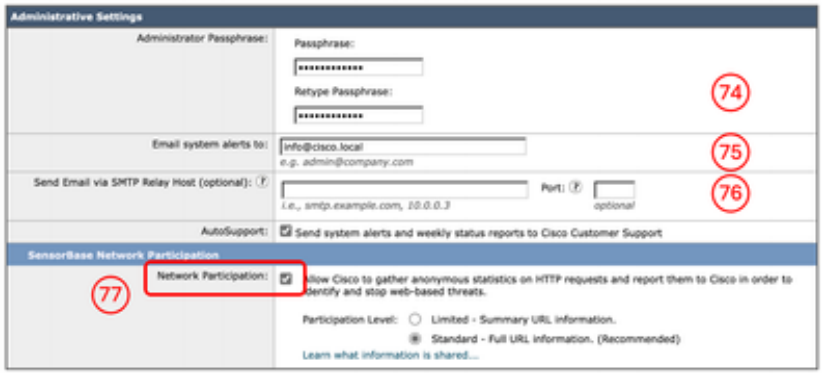


Image - Assistant de configuration du système - Paramètres d'administration

Étape 78. (Facultatif) Vous pouvez modifier les actions par défaut pour la stratégie globale, L4TM, et le filtrage de sécurité des données Cisco, ou vous pouvez les laisser comme valeur par défaut et cliquez sur Suivant.

		Image - Assistant de configuration du système - Paramètres de sécurité Étape 79. Vérifiez votre configuration. Si vous devez apporter des modifications, cliquez sur le bouton Previous pour revenir à la page précédente, ou bien cliquez sur Install This Configuration.

Configuration du réseau

Pour configurer l'interface réseau, vous pouvez utiliser l'interface de ligne de commande ou l'interface utilisateur graphique.

	Commande / Chemin	Action
Configuration des cartes d'interface réseau à partir de CLI	CLI > ifconfig	Nouveau : si l'interface n'est pas répertoriée dans la sortie ifconfig, mais existe dans la machine virtuelle ou l'appliance physique, vous pouvez utiliser cette commande pour afficher l'interface dans la liste. Edit : cette action permet de modifier l'adresse IP, le masque de sous-réseau, le nom d'hôte de l'interface ou d'autres paramètres associés. Details : affiche les détails d'une interface, tels que l'adresse MAC, le type de support, le mode duplex, etc. Delete : supprime l'interface de la liste ifconfig et supprime l'adresse IP si elle a été attribuée précédemment.
Configuration des cartes d'interface réseau depuis l'interface utilisateur	GUI > Réseau > Interfaces	Vous pouvez modifier l'adresse IP et le nom d'hôte de l'interface. Vous pouvez activer, désactiver ou modifier le numéro de port

		du Services de gestion des appareils tels que FTP, SSH, HTTP et HTTPS.

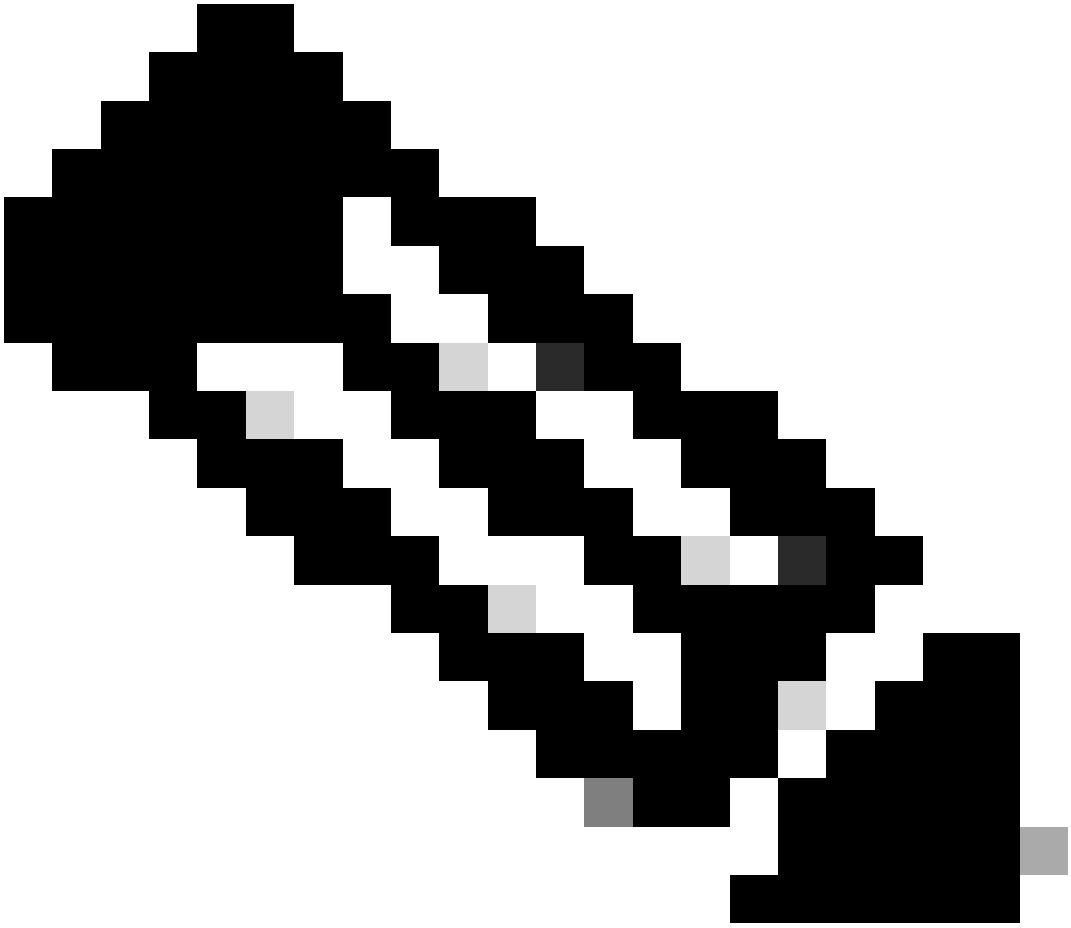
Table de routage

Les routes sont essentielles pour déterminer où diriger le trafic réseau. Le SWA gère ces types de trafic :

- Trafic de données : inclut le trafic traité par le proxy Web à partir d'utilisateurs finaux naviguant sur Internet.
- Trafic de gestion : ce trafic englobe le trafic généré par la gestion de l'appliance via l'interface Web, ainsi que le trafic des services de gestion tels que les mises à niveau SWA, les mises à jour de composants, le DNS, l'authentification et d'autres tâches connexes.

Par défaut, les deux types de trafic utilisent les routes définies pour toutes les interfaces réseau configurées. Cependant, vous avez la possibilité de séparer le routage de sorte que le trafic de gestion utilise une table de routage de gestion dédiée et que le trafic de données utilise une table de routage de données séparée.

Trafic de gestion	Trafic de données
interface utilisateur Web SSH SNMP Authentification, avec contrôleur de domaine (configurable) SYSLOG Push FTP DNS (configurable) Clé de mise à jour/mise à niveau/fonction (configurable)	Proxy HTTP Proxy HTTPS Proxy FTP Négociation WCCP Requête ICAP avec serveur DLP externe DNS (configurable) Clé de mise à jour/mise à niveau/fonction (configurable) Authentification avec contrôleur de domaine (configurable)



Remarque : si vous sélectionnez l'option « Utiliser le port M1 pour la gestion uniquement », une table de routage supplémentaire appelée table de routage des données est ajoutée à la SWA. Cette table de routage ne comporte qu'une seule passerelle par défaut configurable ; tous les chemins de routage supplémentaires doivent être configurés manuellement.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance
- Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Utilisation des meilleures pratiques de sécurisation des appliances Web
- Configurer le pare-feu pour l'appliance Web sécurisée
- Configurer le certificat de déchiffrement dans l'appareil Web sécurisé

- Configuration et dépannage du protocole SNMP dans SWA
- Configuration des journaux de transmission SCP dans l'appliance Web sécurisée avec Microsoft Server
- Activer une chaîne/vidéo YouTube spécifique et bloquer le reste de YouTube dans SWA
- Comprendre le format de journal d'accès HTTPS dans l'appliance Web sécurisée
- Accéder aux journaux de l'appliance Web sécurisée
- Contourner l'authentification dans l'appliance Web sécurisée
- Bloquer le trafic dans l'appliance Web sécurisée
- Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.