Configura installazione iniziale di Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritto come configurare per la prima volta Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.
- Principi fondamentali della rete.

Cisco raccomanda:

- SWA fisico o virtuale installato.
- Accesso amministrativo all'interfaccia grafica (GUI) SWA.
- Accesso amministrativo all'interfaccia CLI (Command Line Interface) SWA.
- Accesso amministrativo alla console SWA.
- Licenza SWA valida o accesso al portale Smart License Management (nel caso si utilizzi

Smart License).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Installazione di SWA

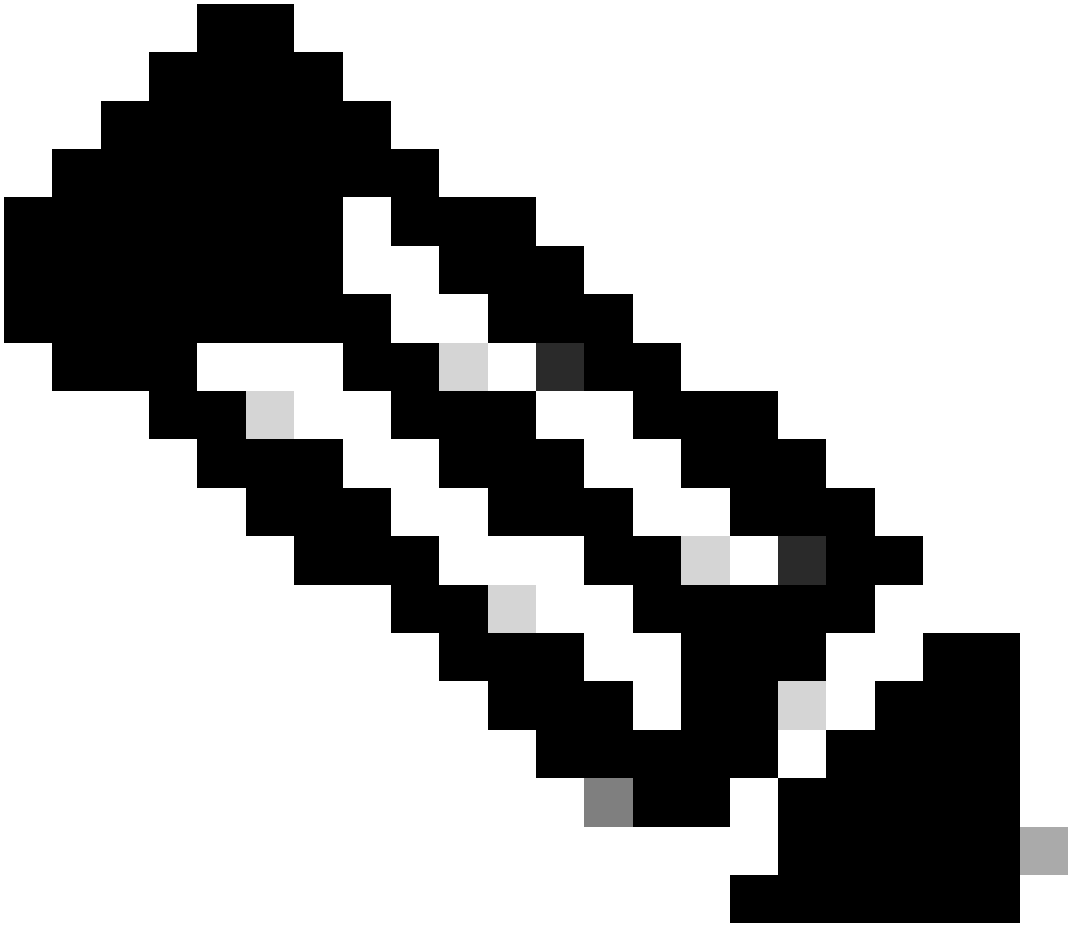
Cisco SWA è una soluzione proxy per il futuro progettata per migliorare la sicurezza e il controllo del Web per le organizzazioni. Disponibile sia in forma fisica che virtuale, l'SWA offre opzioni di installazione flessibili per soddisfare le diverse esigenze. L'interfaccia SWA virtuale supporta diverse piattaforme hypervisor, tra cui Microsoft Hyper-V, VMware ESX e KVM, garantendo la compatibilità con una vasta gamma di ambienti virtuali. Per chi preferisce un dispositivo fisico, Cisco offre tre modelli distinti: S100, S300 e S600. Ogni modello è progettato per soddisfare diversi livelli di prestazioni e requisiti di capacità, garantendo alle organizzazioni la possibilità di trovare la soluzione giusta per le proprie esigenze specifiche di sicurezza Web.

Per scaricare l'immagine della macchina virtuale, visitare: https://software.cisco.com/download/home .

L'installazione dell'interfaccia SWA Cisco virtuale è un processo semplice che inizia con la selezione della piattaforma hypervisor appropriata. Innanzitutto, scaricare il file di installazione SWA virtuale dal sito Web di Cisco. Per VMware ESX, implementare il file OVA, assicurandosi di configurare le impostazioni di rete e di allocare risorse sufficienti quali CPU, memoria e storage. Per Microsoft Hyper-V, importare il file VHD scaricato nella console di gestione di Hyper-V e configurare di conseguenza le impostazioni della macchina virtuale. Per i sistemi KVM, utilizzare lo strumento da riga di comando virt-manager o virsh per definire e avviare la macchina virtuale utilizzando l'immagine scaricata. Una volta che la macchina virtuale è attiva e in esecuzione, è possibile eseguire la configurazione iniziale seguendo i passaggi descritti in questo articolo.

Configurazione iniziale

Dopo aver installato l'SWA, procedere con questi passaggi per la distribuzione iniziale.



Nota: per la configurazione iniziale, è necessario avere accesso a SWA tramite console, SSH e GUI.

Metodo Connection	Fase	Procedura di configurazione
Console	Configura indirizzo IP	Passaggio 1. Immettere il nome utente e la password per accedere alla CLI.

Suggerimento: il nome utente predefinito è admin e la password predefinita è ironport.

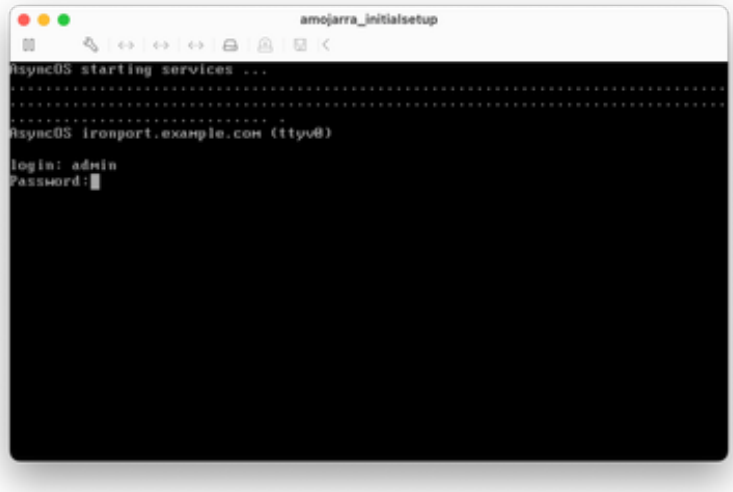


Immagine - schermata di accesso

Passaggio 2. Eseguire il comando ifconfig.

Passaggio 3. Scegliere Modifica.

Passaggio 4. Inserire il numero associato all'interfaccia di gestione.

Passaggio 5. Selezionare Y per modificare l'indirizzo IPv4 predefinito.

Passaggio 6. Immettere l'indirizzo IP

Passaggio 7. Immettere la subnet mask.

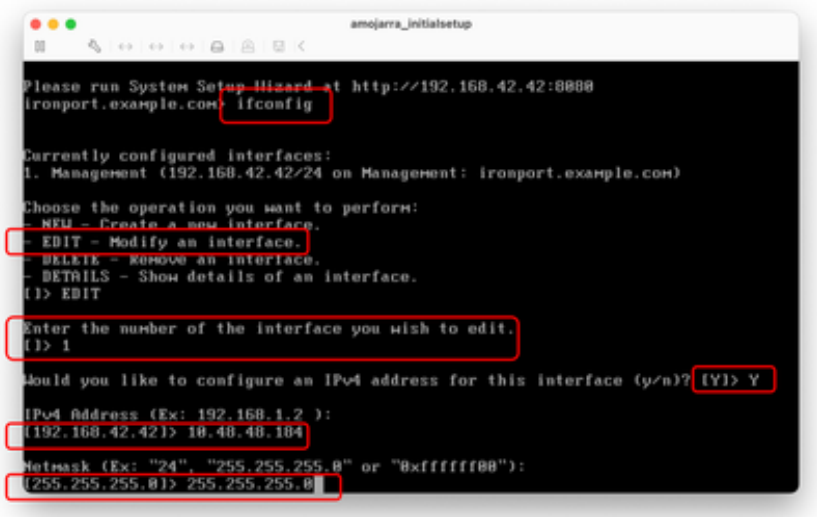


Immagine - Modifica indirizzo IP interfaccia di gestione

Passaggio 8. Se si desidera configurare IPv6, digitare Y in risposta alla domanda "Configurare IPv6?", altrimenti è possibile mantenere l'impostazione predefinita (No) e premere Invio.

Passaggio 9. Immettere un nome di dominio completo (FQDN) come nome host.

Passaggio 10. Per abilitare l'accesso FTP (File Transfer Protocol) all'interfaccia di gestione, scegliere S oppure Invio.

Passaggio 11. Per impostazione predefinita, Secure Shell (SSH) è abilitata. Si consiglia di abilitare SSH. Digitare Y per continuare.

Passaggio 12. (Facoltativo) È possibile modificare la porta SSH predefinita da TCP 22 a qualsiasi numero di porta si desideri, a condizione che non vi siano conflitti di porte. Per utilizzare la porta predefinita (TCP/22), premere Invio.

Passaggio 13. Se si desidera disporre dell'accesso HTTP (Hypertext Transfer Protocol) all'interfaccia di gestione, digitare Y e impostare il numero di porta per l'accesso HTTP. In caso contrario, è possibile scegliere N per disporre solo dell'accesso HTTPS (Hypertext Transfer Protocol Secure) all'interfaccia di gestione.

Passaggio 14. Digitare Y e premere Invio per abilitare

l'accesso HTTPS all'interfaccia di gestione.

Passaggio 15. È possibile modificare il numero di porta HTTPS predefinito da 8443 a qualsiasi numero di porta desiderato, a condizione che non vi siano altri conflitti di porte. Premere Invio per utilizzare la porta predefinita (TCP/8443).

Passaggio 16. L'API (Application Programming Interface) per impostazione predefinita è impostata su Abilita. Se non si utilizza l'API, è possibile disabilitarla digitando N e premendo Invio.

Passaggio 17. Se si sceglie di abilitare l'API, è possibile modificare il numero di porta predefinito dell'API da 6080 a qualsiasi numero di porta desiderato, purché non si verifichino altri conflitti di porta. Premere invio per utilizzare la porta predefinita (TCP/6080).

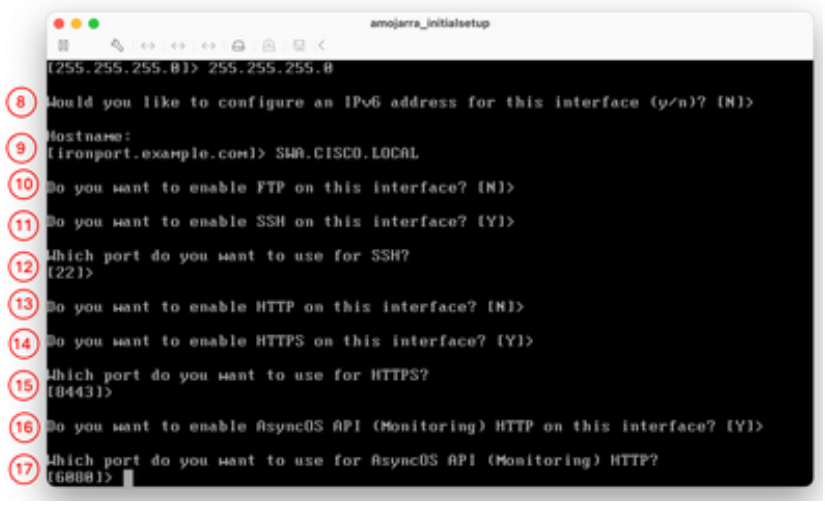
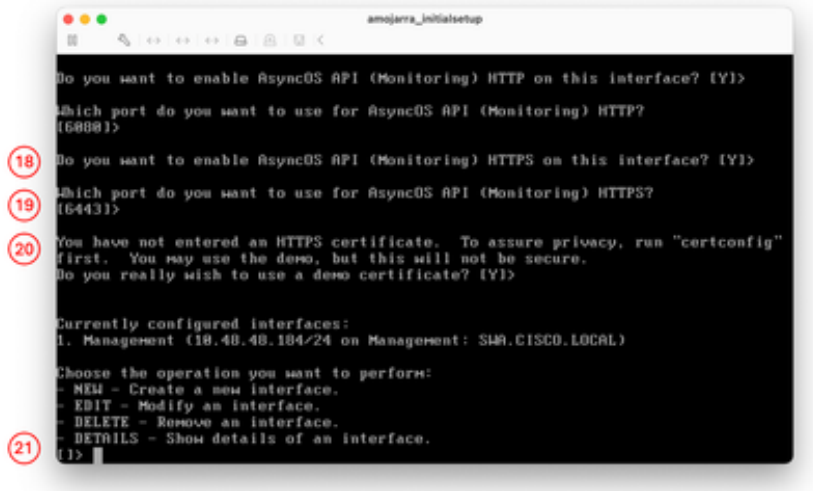


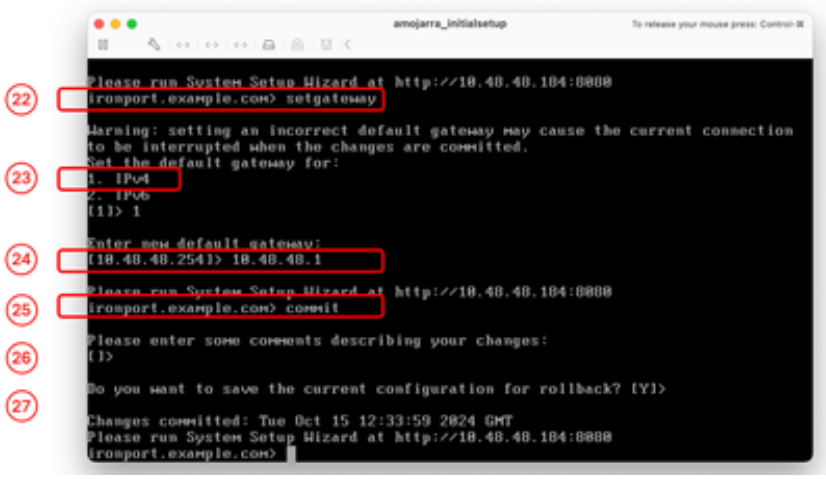
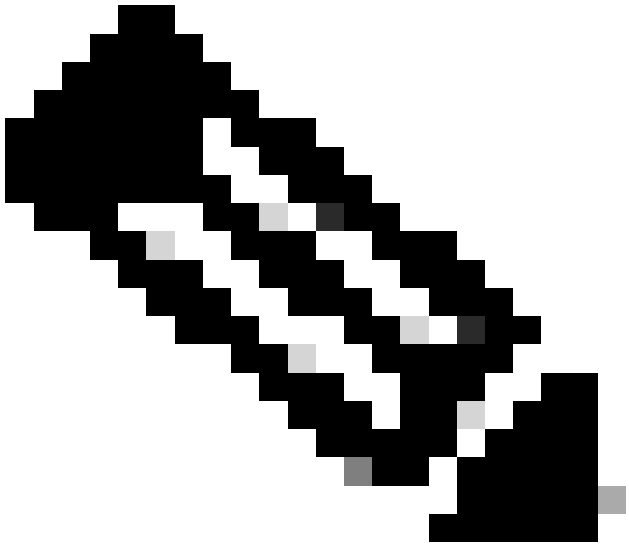
Immagine - Configurazione servizio interfaccia di gestione

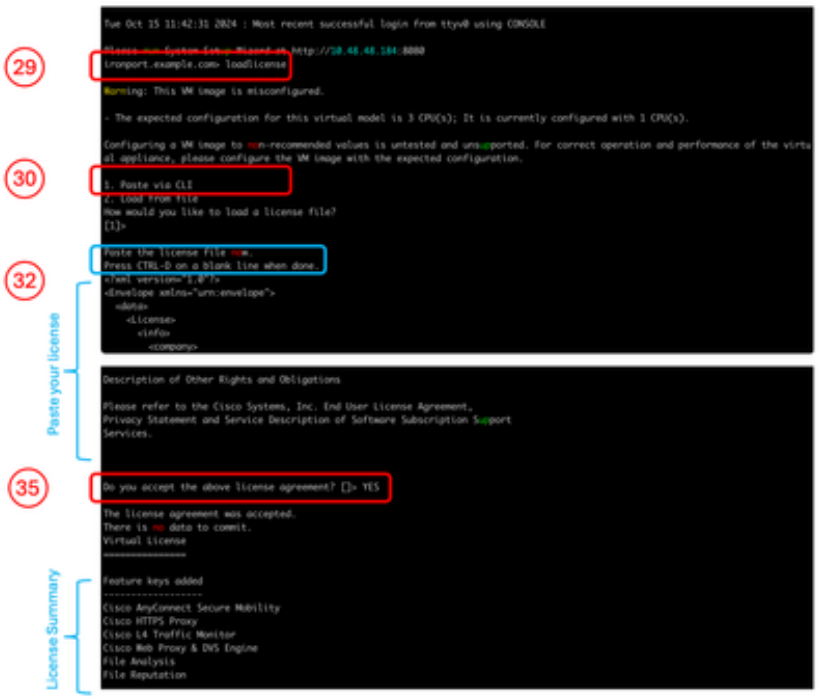
Passaggio 18. L'API AsyncOS (monitoraggio) è la nuova GUI del pannello SWA. Se si desidera utilizzare i nuovi rapporti dell'interfaccia utente, impostare questa opzione su Y (predefinito). In caso contrario, digitare N e andare al punto 20.

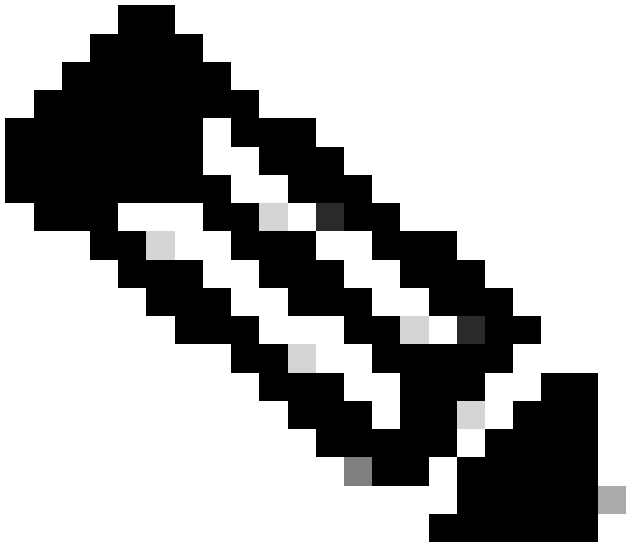
Passaggio 19. È possibile modificare il numero di porta HTTPS predefinito della nuova GUI da 6443 a qualsiasi numero di porta desiderato, purché non vi siano altri conflitti di porte. Premere Invio per utilizzare la porta predefinita (TCP/6443).

Passaggio 20. L'interfaccia di gestione SWA utilizza un certificato demo Cisco. Digitare Y per accettare il

		certificato demo. è possibile modificare il certificato GUI dopo la configurazione iniziale. Passaggio 21. Premere Invio per uscire dalla procedura guidata ifconfig.  Immagine - Nuova configurazione GUI TCP
	Configura gateway predefinito	Passaggio 22. Eseguire setgateway. Passaggio 23. Scegliere IPv4 se l'interfaccia di gestione è stata configurata con IPv4, altrimenti scegliere IPv6. Passaggio 24. Immettere l'indirizzo IP del gateway predefinito. Passaggio 25. Salvare le modifiche eseguendo il commit. Passaggio 26. (Facoltativo) è possibile aggiungere note sulle modifiche da salvare Passaggio 27. (Facoltativo) è possibile disporre di un file SWA per eseguire il backup della configurazione prima di applicare le modifiche.

		 Immagine - Configurazione del gateway predefinito
SSH	Importa licenza tradizionale	 Nota: se si utilizza Smart License, andare al passo 36. Passaggio 28. Collegare il dispositivo SWA tramite SSH. Passaggio 29. Esegui loadlicense Passaggio 30. Scegliere Incolla tramite CLI. Passaggio 31. Aprire il file di licenza con un editor di testo e copiarne tutto il contenuto Passaggio 32. Incollare la licenza nella shell SSH. Passaggio 33. Premere Invio per passare a una nuova

		riga. Passaggio 34. Tenere premuto Control e premere D. Passaggio 35. Leggere il Contratto di Licenza e digitare YES per accettare le condizioni.  Immagine - Importa licenza tradizionale Andare al passo 58.
GUI	Configura server DNS	Passaggio 37. Accedere alla GUI (l'impostazione predefinita è HTTPS://<FQDN SWA o indirizzo IP>:8443) Passaggio 38. Passare alla rete e scegliere DNS. Passaggio 39. Fare clic su Modifica impostazioni. Passaggio 40. Nella sezione Server DNS primari selezionare Utilizza questi server DNS. Passaggio 41. Impostare Priorità su 0 e immettere l'indirizzo IP del server DNS.



Nota: è possibile aggiungere più server DNS scegliendo Aggiungi riga.

Passaggio 42. Invia.

Passaggio 43. Eseguire il commit delle modifiche.

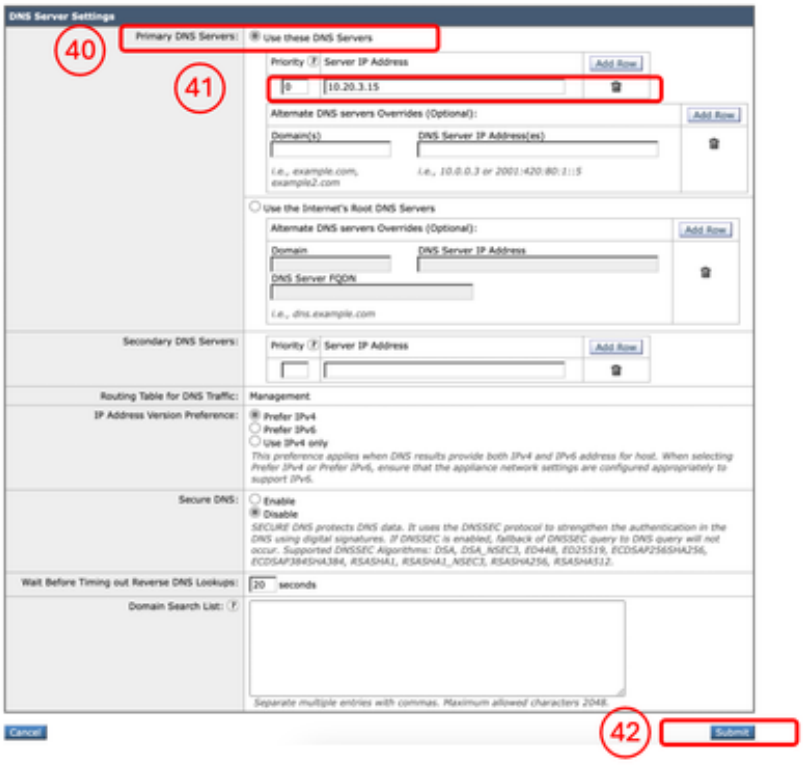
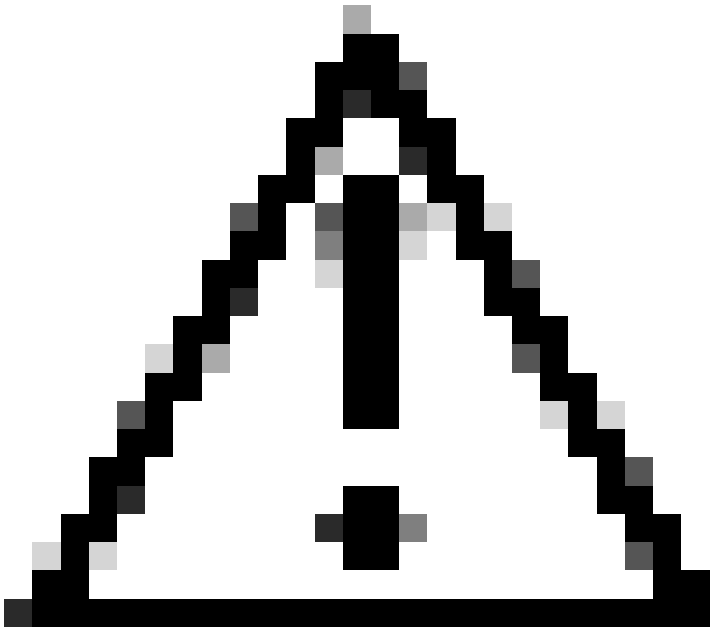


Immagine - Configurazione server DNS

	Configura Smart License	Passaggio 44. Nell'interfaccia utente di Amministrazione sistema, scegliere Licenze software Smart. Passaggio 45. Scegliere Enable Smart Software Licensing.  Attenzione: dopo aver attivato la funzione Smart License sull'accessorio, non è possibile eseguire il rollback da Smart License a Classic License. Passaggio 46. Fare clic su OK per continuare la configurazione di Smart License. Passaggio 47. Eseguire il commit delle modifiche. Passaggio 48. Per ottenere il token per registrare il tuo SWA, accedi a Cisco Software Central (https://software.cisco.com/#) Passaggio 49. Fare clic su Gestisci licenze.

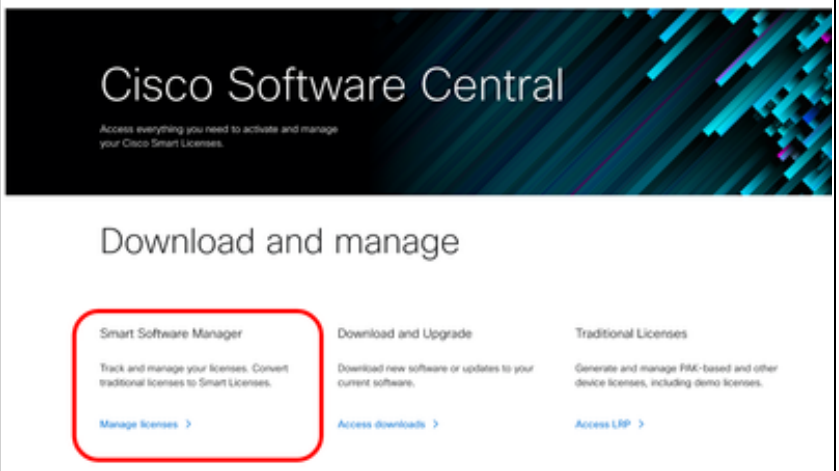


Immagine - Gestione licenze Cisco Smart

Passaggio 50. In Licenze Smart Software scegliere Inventario.

Passaggio 51. Nella scheda General, creare un nuovo token o usare i token disponibili.

Immagine - Pagina Inventario delle licenze di Smart Software

Passaggio 52. Immettere le informazioni richieste e creare il token.

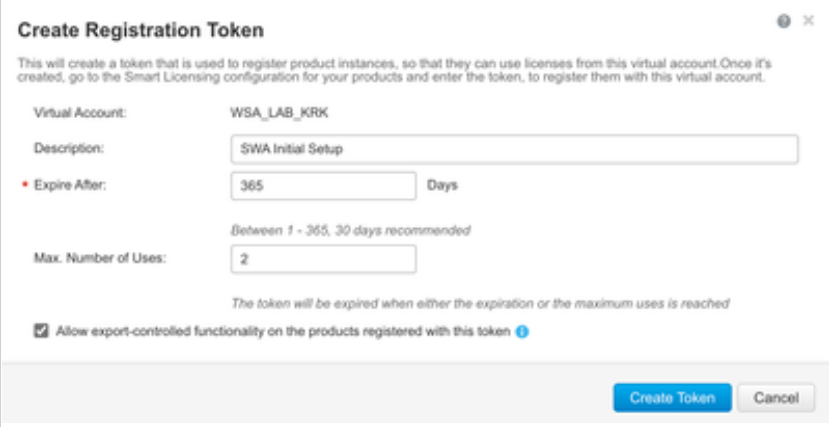


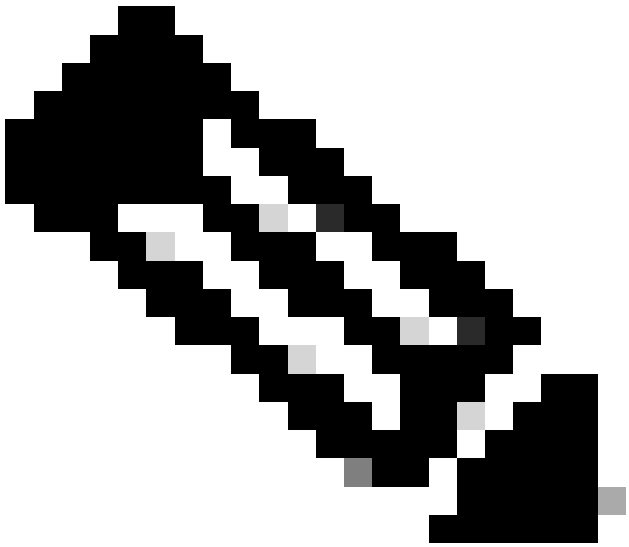
Immagine - Generazione di un token

Passaggio 53. Fare clic sull'icona blu davanti al token

appena aggiunto e copiarne il contenuto.

Immagine - Copia il token

Passaggio 54. Nell'interfaccia grafica SWA, selezionare System Administration (Amministrazione sistema), quindi Smart Software Licensing (Licenze software intelligente).



Nota: se si è già nella pagina Licenze Smart Software, aggiornare la pagina.

Passaggio 55. (Facoltativo) Se l'SWA non dispone di accesso a Internet dall'interfaccia di gestione, è possibile modificare l'interfaccia di test specificando le interfacce a cui è consentito accedere a Internet.

Suggerimento: per ulteriori informazioni sulla configurazione di più interfacce e sulle tabelle di routing, consultare la sezione Configurazione di rete in questo articolo.

Passaggio 56. Fare clic su Registra.

Passaggio 57. Incollare il token e fare clic su Register.

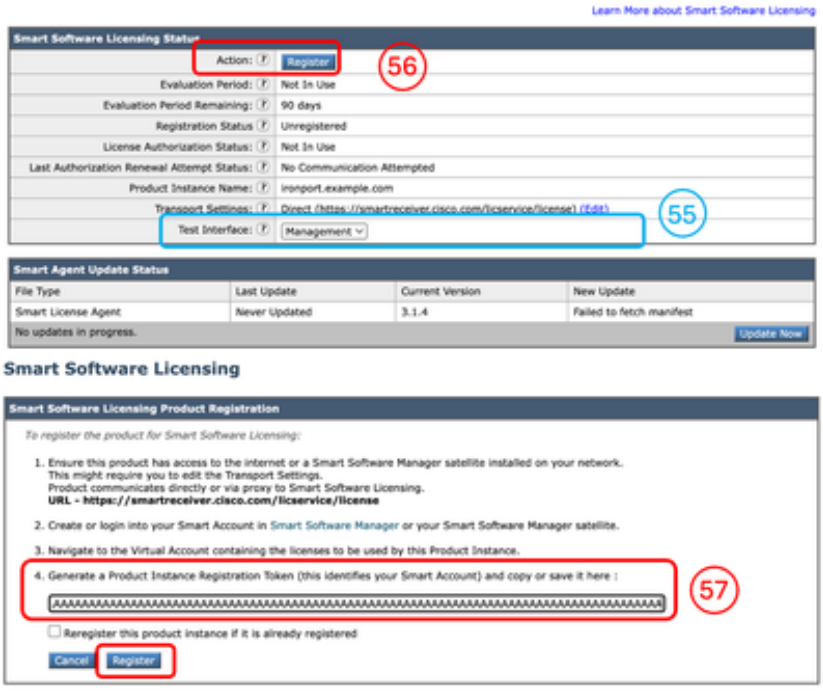
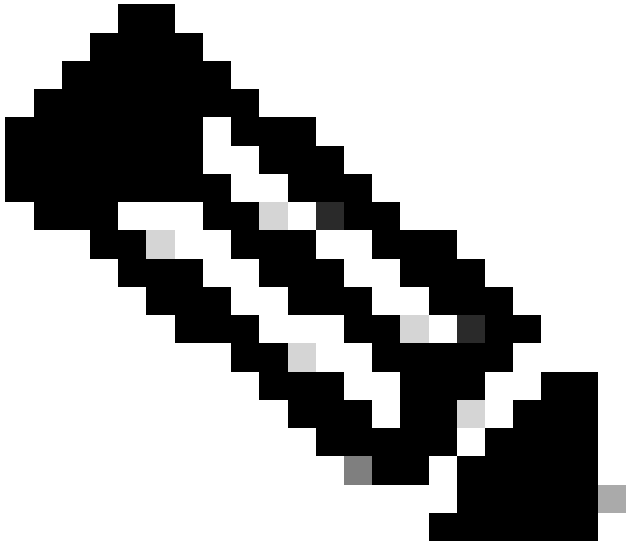
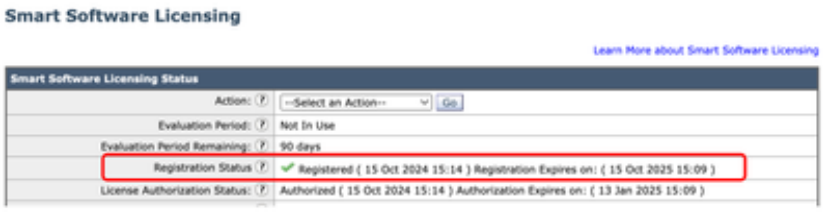
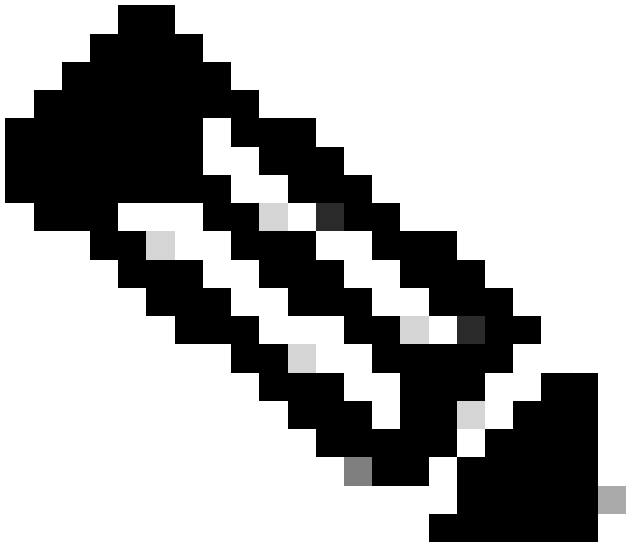
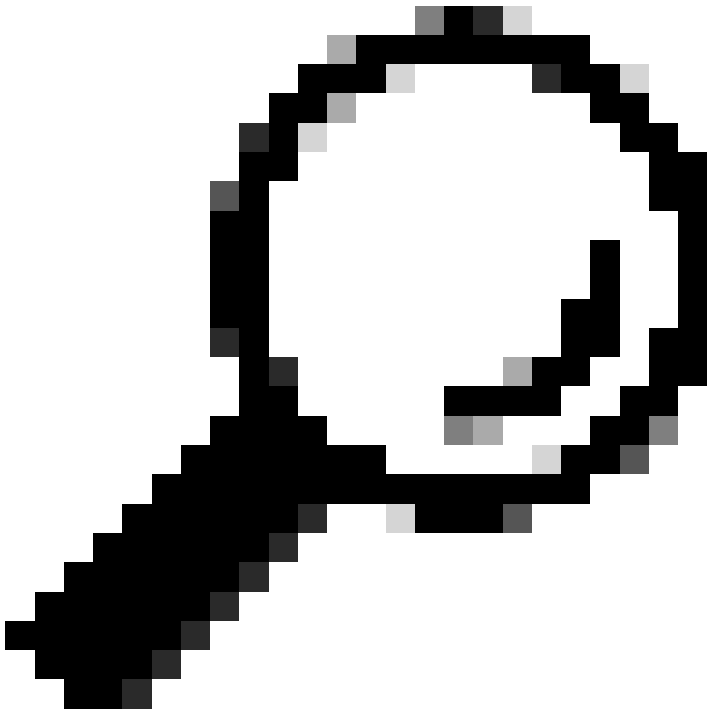


		Immagine - Registrazione SWA su Smart License  Nota: per verificare la registrazione, attendere alcuni minuti, aggiornare la pagina Smart Licensing in SWA e controllare lo stato della registrazione.  Immagine - Stato di registrazione della licenza Smart
	Configurazione guidata sistema	Passaggio 58. Nell'interfaccia grafica SWA, passare a System Administration (Amministrazione sistema) e scegliere System Setup Wizard (Configurazione guidata sistema). Passaggio 59. Leggere e accettare i termini del presente contratto di licenza Passaggio 60. Fare clic su Inizia installazione. Passaggio 61. Scegli Standard dal Sezione Modalità di funzionamento dell'accessorio. Passaggio 62. Immettere il nome host predefinito del sistema.

		 Nota: il nome host precedente creato nel passo 9 era correlato all'interfaccia di gestione e non all'interfaccia SWA. Passaggio 63. Immettere l'indirizzo IP dei server DNS. Passaggio 64. è possibile configurare il server Network Time Protocol (NTP).  Suggerimento: se il server NTP richiede

l'autenticazione, è possibile configurare i parametri Key.

Passaggio 65. Selezionare il fuso orario che si applica all'SWA e fare clic su Avanti.

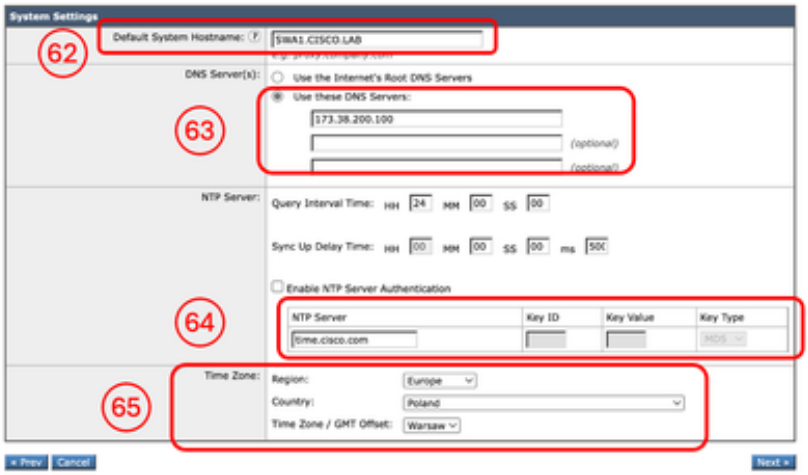


Immagine - Configurazione guidata sistema - Impostazioni di sistema

Passaggio 66. (Facoltativo) Se si utilizza un proxy upstream nella rete, è possibile configurarlo nella pagina Contesto di rete oppure lasciarlo come predefinito e fare clic su Avanti.

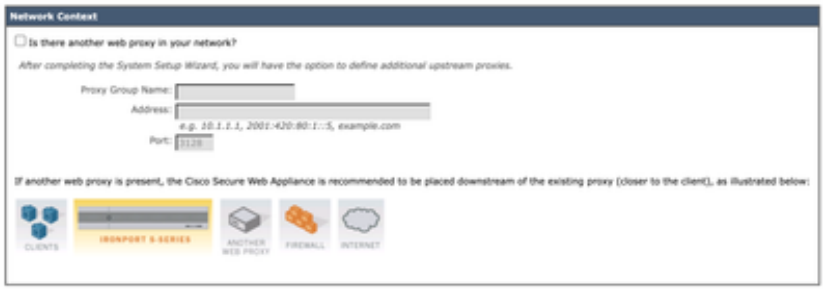


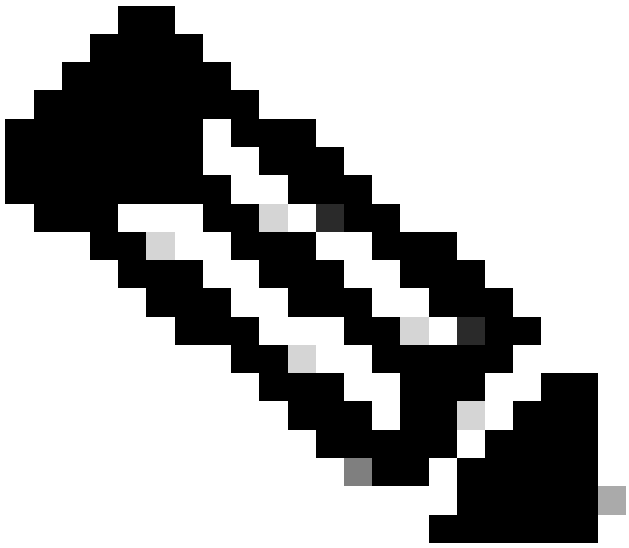
Immagine - Configurazione guidata sistema - Configurazione proxy upstream

Passaggio 67. (Facoltativo) Se è necessario separare il traffico nell'interfaccia di gestione dal traffico nelle interfacce dati (interfacce P1 e P2), selezionare Usa porta M1 solo per la gestione.

Passaggio 68. (Facoltativo) È possibile aggiungere o modificare l'indirizzo IP delle interfacce di rete dalla sezione Indirizzo IPv4/Netmask o Indirizzo IPv6/Netmask.

Passaggio 69. (Facoltativo) È possibile aggiungere o modificare il nome host delle interfacce di rete e fare clic

su Avanti.



Nota: la porta P1 può essere abilitata e configurata tramite la Configurazione guidata del sistema. Se si desidera attivare l'interfaccia P2, eseguire questa operazione dopo aver completato la Configurazione guidata sistema.

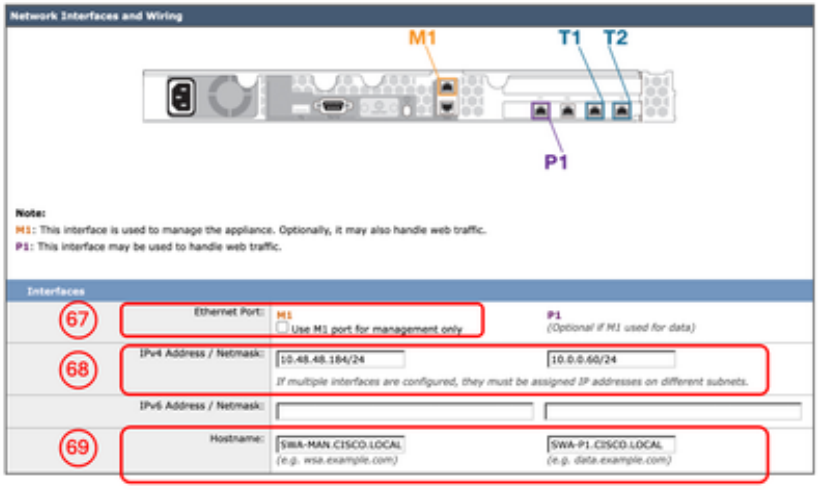


Immagine - Configurazione guidata del sistema - Configurazione delle interfacce di rete

Passaggio 70. (Facoltativo) Se si intende configurare il monitoraggio del traffico di layer 4 (L4TM), è possibile configurare l'impostazione duplex oppure mantenere l'impostazione predefinita e fare clic su Avanti.

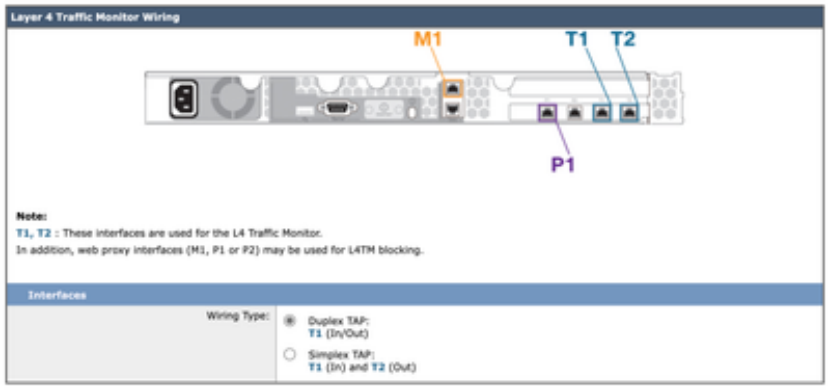
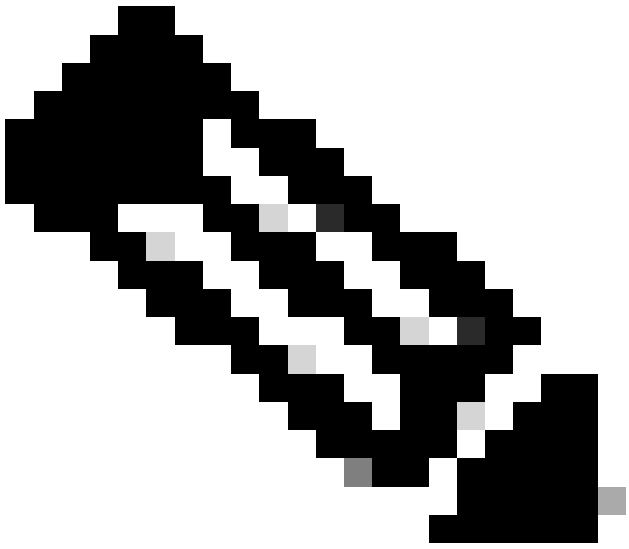


Immagine - Configurazione guidata sistema - Impostazione Monitor traffico Layer 4

Passaggio 71. (Facoltativo) Nella pagina Route IPv4 per la gestione è possibile modificare il gateway predefinito

Passaggio 72. (Facoltativo) È possibile aggiungere un instradamento per creare instradamenti statici.



Nota: se si sceglie "Usa porta M1 solo per la gestione" nel passo 67, esisteranno due tabelle di routing separate per l'interfaccia di gestione e le interfacce dati (P1 e P2).

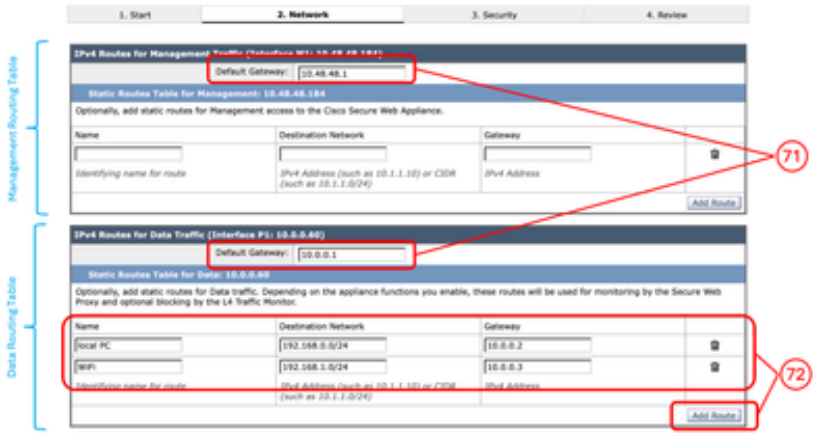


Immagine - Configurazione guidata sistema - Aggiungi route

Passaggio 73. (Facoltativo) Se si desidera configurare la distribuzione di proxy trasparente, tramite il protocollo WCCP (Web Cache Communication Protocol), è possibile configurare le impostazioni WCCP oppure lasciare invariato lo switch di layer 4 predefinito e fare clic su Avanti.

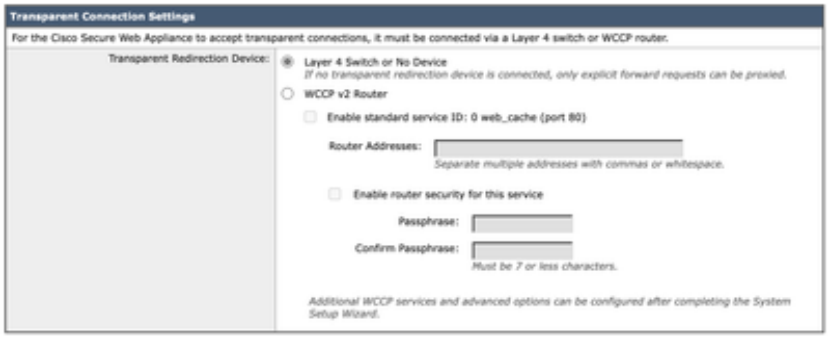


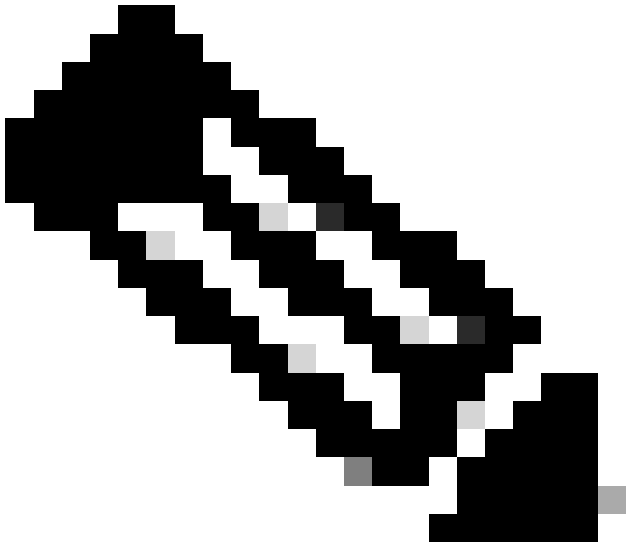
Immagine - Installazione guidata sistema - Configurazione distribuzione proxy

Passaggio 74. Impostare una nuova password per l'account admin.

Passaggio 75. Immettere un indirizzo di posta elettronica al quale si prevede di ricevere gli avvisi di sistema.

Passaggio 76. (Facoltativo) Fornire le informazioni sull'host del relay Simple Mail Transfer Protocol (SMTP), altrimenti lasciarle vuote Se non è definito alcun host di inoltro interno, SMTP utilizza la ricerca DNS del record MX.

Passaggio 7. (Facoltativo) Se si desidera disabilitare la partecipazione alla rete Cisco SensorBase, deselezionare la casella di controllo Partecipazione alla rete, altrimenti lasciare inalterato il valore predefinito e fare clic su Avanti.



Nota: la partecipazione a Cisco SensorBase Network implica che Cisco raccoglie i dati e li condivide con il database di gestione delle minacce di SensorBase.

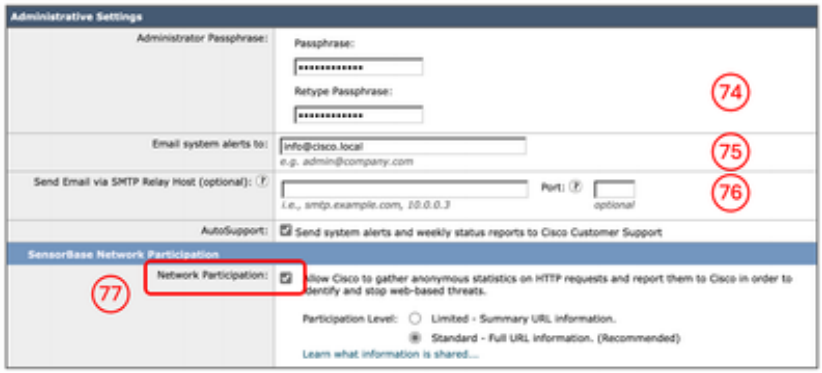


Immagine - Configurazione guidata sistema - Impostazioni amministrative

Passaggio 78. (Facoltativo) È possibile modificare le azioni predefinite per Criteri globali, L4TM e Cisco Data Security Filtering, oppure è possibile lasciarle come predefinite e fare clic su Avanti.

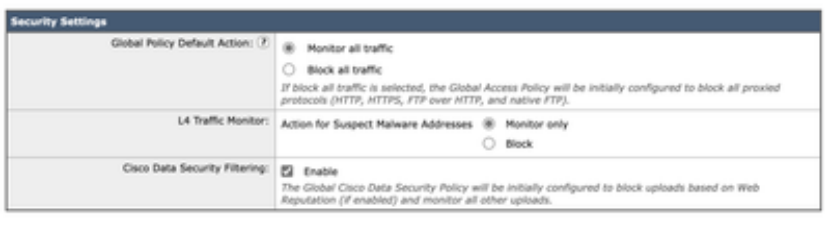


Immagine - Configurazione guidata sistema - Impostazioni protezione

		Passaggio 79. Verificare la configurazione. Se è necessario apportare modifiche, fare clic sul pulsante Precedente per tornare alla pagina precedente oppure fare clic su Installa questa configurazione.

Configurazione della rete

Per configurare l'interfaccia di rete è possibile usare sia la CLI che la GUI.

	Comando/Percorso	Azione
Configurazione delle schede di interfaccia di rete dalla CLI	CLI >ifconfig	Novità: se l'interfaccia non è elencata nell'output ifconfig, ma è presente nella macchina virtuale o nell'accessorio fisico, è possibile utilizzare questo comando per visualizzare l'interfaccia nell'elenco. Modifica: questa azione consente di modificare l'indirizzo IP, la subnet mask, il nome host dell'interfaccia o altri parametri correlati. Dettagli: visualizza i dettagli di un'interfaccia, ad esempio l'indirizzo MAC, il tipo di supporto, la modalità duplex e così via. Delete: rimuove l'interfaccia dall'elenco ifconfig e rimuove l'indirizzo IP se assegnato in precedenza.
Configurazione delle schede di interfaccia di rete dalla GUI	GUI >Rete > Interfacce	È possibile modificare l'indirizzo IP e il nome host dell'interfaccia. È possibile abilitare, disabilitare o modificare il numero di porta del Servizi di gestione degli

		accessori quali FTP, SSH, accesso HTTP e accesso HTTPS.

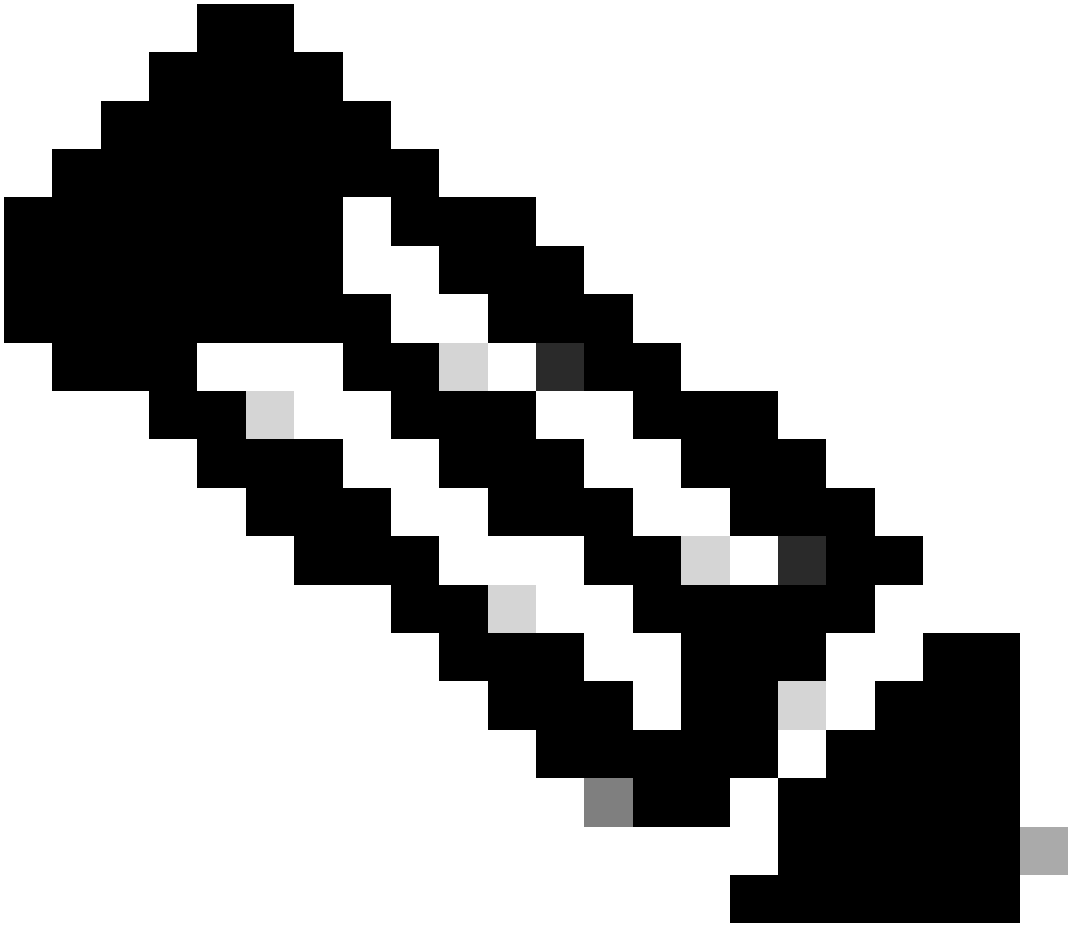
Tabella di routing

Le route sono essenziali per determinare dove indirizzare il traffico di rete. L'SWA gestisce questi tipi di traffico:

- Traffico dati: comprende il traffico elaborato dal proxy Web dagli utenti finali che navigano su Internet.
- Traffico di gestione: comprende il traffico generato dalla gestione dell'accessorio tramite l'interfaccia Web, nonché il traffico per servizi di gestione quali aggiornamenti SWA, aggiornamenti di componenti, DNS, autenticazione e altre attività correlate.

Per impostazione predefinita, entrambi i tipi di traffico utilizzano le route definite per tutte le interfacce di rete configurate. È tuttavia possibile separare il routing in modo che il traffico di gestione utilizzi una tabella di routing di gestione dedicata e il traffico di dati utilizzi una tabella di routing di dati separata.

Traffico di gestione	Traffico di dati
Interfaccia Web SSH SNMP Autenticazione, con controller di dominio (configurabile) Syslog push FTP DNS (configurabile) Chiave di aggiornamento/aggiornamento/funzionalità (configurabile)	Proxy HTTP Proxy HTTPS Proxy FTP Negoziazione WCCP Richiesta ICAP con server DLP esterno DNS (configurabile) Chiave di aggiornamento/aggiornamento/funzionalità (configurabile) Autenticazione con controller di dominio (configurabile)



Nota: se si seleziona l'opzione "Usa porta M1 solo per la gestione", all'SWA viene aggiunta una tabella di routing aggiuntiva denominata tabella di routing dei dati. Questa tabella di routing ha un solo gateway predefinito configurabile; tutti i percorsi di routing aggiuntivi devono essere configurati manualmente.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance
- Guida all'installazione di Cisco Secure Email e Web Virtual Appliance
- Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco
- Utilizzare le procedure ottimali per Secure Web Appliance
- Configurare il firewall per Secure Web Appliance
- Configura certificato di decrittografia in Appliance Web sicura

- Configurazione e risoluzione dei problemi di SNMP in SWA
- Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server
- Abilita canale/video YouTube specifico e blocca resto di YouTube in SWA
- Informazioni sul formato HTTPS Accesslog in Secure Web Appliance
- Accesso ai registri protetti di Web Appliance
- Ignora autenticazione in Secure Web Appliance
- Blocca il traffico in Secure Web Appliance
- Ignora traffico aggiornamenti Microsoft in Secure Web Appliance

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).