Ersteinrichtung der sicheren Webappliance konfigurieren

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur erstmaligen Konfiguration der Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.
- Grundlegende Netzwerkgrundsätze

Cisco empfiehlt Folgendes:

- Installierte physische oder virtuelle SWA.
- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administrator-Zugriff auf die SWA-Befehlszeilenschnittstelle (CLI)
- Administratorzugriff auf die SWA-Konsole.
- Gültige SWA-Lizenz oder Zugriff auf das Smart License Management-Portal (falls Sie Smart

License verwenden).

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

SWA installieren

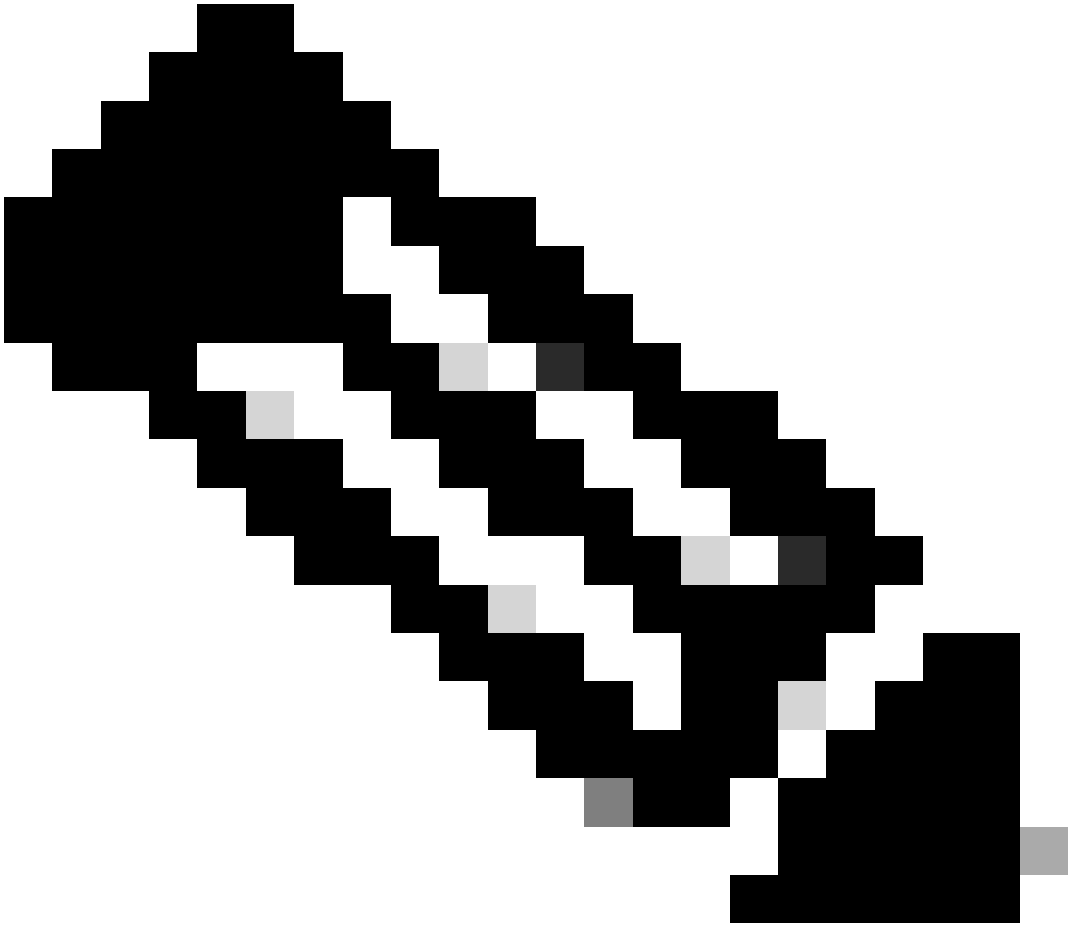
Die Cisco SWA ist eine Forward Proxy-Lösung zur Optimierung der Web-Sicherheit und -Kontrolle für Unternehmen. Die SWA sind sowohl in virtueller als auch in physischer Form erhältlich und bieten flexible Bereitstellungsoptionen für die unterschiedlichsten Anforderungen. Das virtuelle SWA unterstützt mehrere Hypervisor-Plattformen, darunter Microsoft Hyper-V, VMware ESX und KVM, sodass die Kompatibilität mit einer Reihe virtueller Umgebungen gewährleistet ist. Für Kunden, die eine physische Appliance bevorzugen, bietet Cisco drei verschiedene Modelle: S100, S300 und S600. Jedes Modell ist auf unterschiedliche Leistungs- und Kapazitätsanforderungen ausgelegt, um sicherzustellen, dass Unternehmen die richtige Lösung für ihre spezifischen Web-Sicherheitsanforderungen finden.

Um Ihr VM-Image herunterzuladen, besuchen Sie: https://software.cisco.com/download/home .

Die Installation der virtuellen Cisco SWA ist ein einfacher Prozess, der mit der Auswahl der geeigneten Hypervisor-Plattform beginnt. Laden Sie zunächst die virtuelle SWA-Installationsdatei von der Cisco Website herunter. Stellen Sie für VMware ESX die OVA-Datei bereit, und stellen Sie sicher, dass Sie die Netzwerkeinstellungen konfigurieren und ausreichende Ressourcen wie CPU, Speicher und Speicher zuweisen. Importieren Sie für Microsoft Hyper-V die heruntergeladene VHD-Datei in den Hyper-V Manager, und konfigurieren Sie die Einstellungen der virtuellen Maschine entsprechend. Verwenden Sie für KVM das Befehlszeilentool virt-manager oder virsh, um das virtuelle System mithilfe des heruntergeladenen Images zu definieren und zu starten. Sobald die virtuelle Maschine in Betrieb ist, können Sie die Schritte in diesem Artikel verwenden, um die Ersteinrichtung durchzuführen.

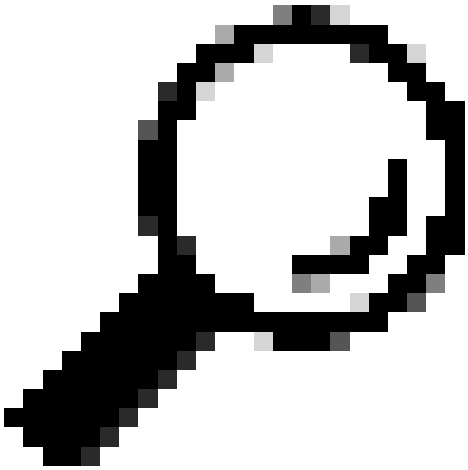
Ersteinrichtung

Fahren Sie nach der SWA-Installation mit den folgenden Schritten für die Erstbereitstellung fort.



Hinweis: Für die Ersteinrichtung benötigen Sie Zugriff auf SWA über Konsole, SSH und GUI.

Verbindungsmethode	Phase	Konfigurationsschritte
Konsole	IP-Adresse konfigurieren	Schritt 1: Geben Sie den Benutzernamen und das Passwort für die Anmeldung bei der CLI ein.



Tipp: Der Standard-Benutzername lautet admin, und das Standard-Kennwort lautet ironport.

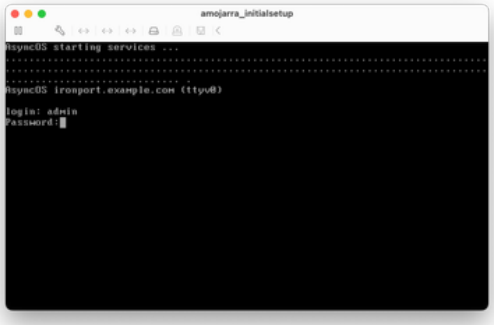


Bild - Anmeldebildschirm

Schritt 2: Führen Sie ifconfig aus.

Schritt 3: Wählen Sie Bearbeiten aus.

Schritt 4: Geben Sie die Nummer ein, die Ihrer Verwaltungsschnittstelle zugeordnet ist.

Schritt 5: Wählen Sie Y aus, um die Standard-IPv4-Adresse zu bearbeiten.

Schritt 6: Geben Sie die IP-Adresse ein

Schritt 7. Geben Sie die Subnetzmaske ein.

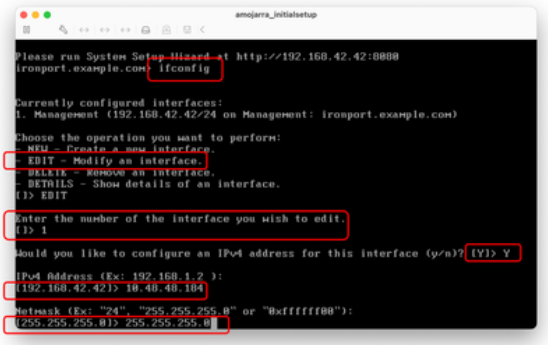


Bild - IP-Adresse der Management-Schnittstelle bearbeiten

Schritt 8: Wenn Sie IPv6 konfigurieren möchten, geben Sie Y in Antwort auf die Frage "Möchten Sie IPv6 konfigurieren?" ein. Andernfalls können Sie dies als Standard (Nein) beibehalten und die Eingabetaste drücken.

Schritt 9. Geben Sie einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) als Hostnamen ein.

Schritt 10. Wenn Sie das File Transfer Protocol (FTP)-Zugriffs-Protokoll auf die Verwaltungsschnittstelle aktivieren möchten, wählen Sie Y aus, oder drücken Sie die Eingabetaste.

Schritt 11. Die Secure Shell (SSH) ist standardmäßig auf Enabled (Aktiviert) festgelegt. Es wird empfohlen, SSH zu aktivieren. Geben Sie Y ein, um fortzufahren.

Schritt 12: (Optional) Sie können den Standard-SSH-Port von TCP 22 auf jede gewünschte Port-Nummer ändern, solange es keine anderen Port-Konflikte gibt. Drücken Sie die Eingabetaste, um den Standard-Port (TCP/22) zu verwenden.

Schritt 13: Wenn Sie über HTTP-Zugriff (Hypertext Transfer Protocol) auf die Verwaltungsschnittstelle

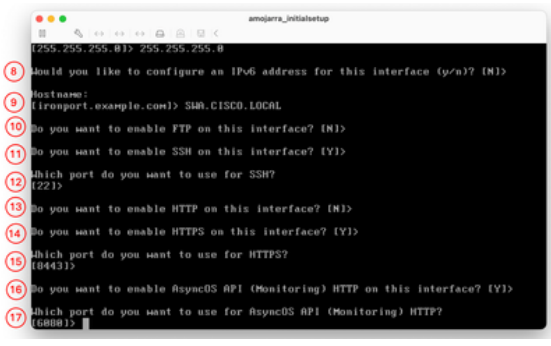
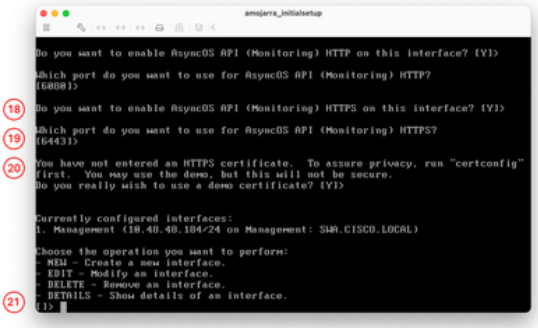
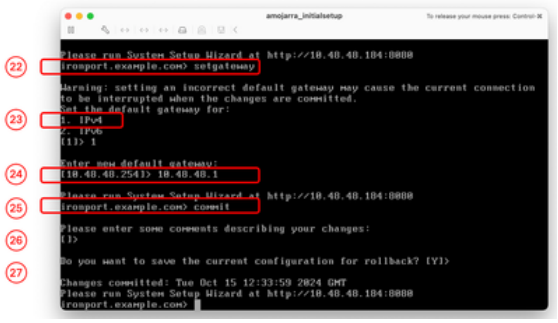
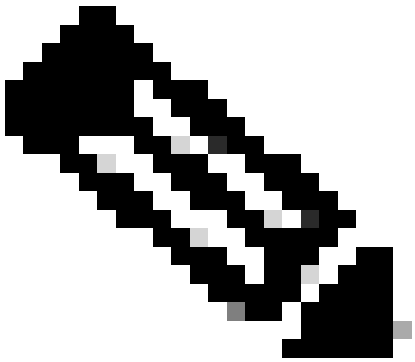
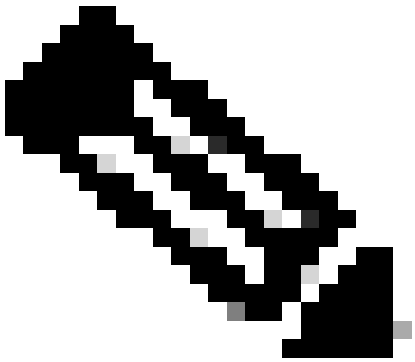
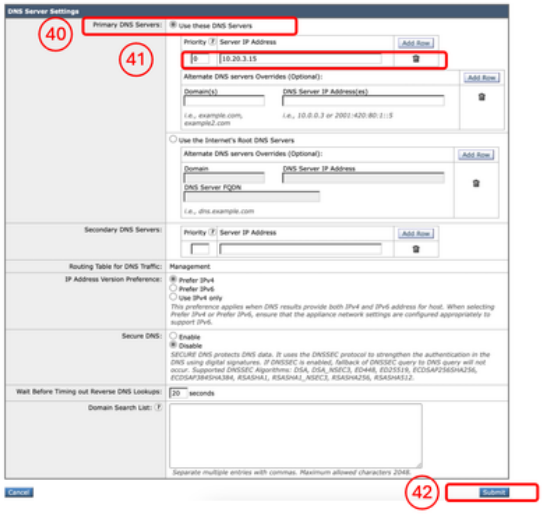
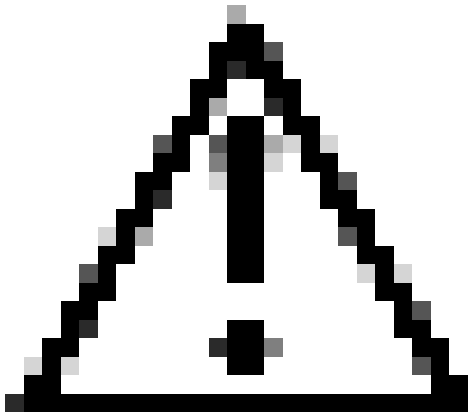
		verfügen möchten, geben Sie Y ein, und legen Sie die Portnummer für den HTTP-Zugriff fest. Andernfalls können Sie N auswählen, um nur über HTTPS (Hypertext Transfer Protocol Secure) auf die Verwaltungsschnittstelle zuzugreifen. Schritt 14: Geben Sie Y ein, und drücken Sie die Eingabetaste, um den HTTPS-Zugriff auf die Verwaltungsschnittstelle zu aktivieren. Schritt 15: Sie können die Standard-HTTPS-Portnummer von 8443 in jede gewünschte Portnummer ändern, solange es keine Portkonflikte gibt. Drücken Sie die Eingabetaste, um den Standard-Port (TCP/8443) zu verwenden. Schritt 16: Application Programming Interface (API) ist standardmäßig auf Enable (Aktivieren) eingestellt. Wenn Sie keine API verwenden, können Sie die API deaktivieren, indem Sie N eingeben und die Eingabetaste drücken. Schritt 17: Wenn Sie die API aktiviert haben, können Sie die standardmäßige API-Portnummer von 6080 auf jede gewünschte Port-Nummer ändern, solange es keine anderen Port-Konflikte gibt. Drücken Sie die Eingabetaste, um den Standardport (TCP/6080) zu verwenden. 

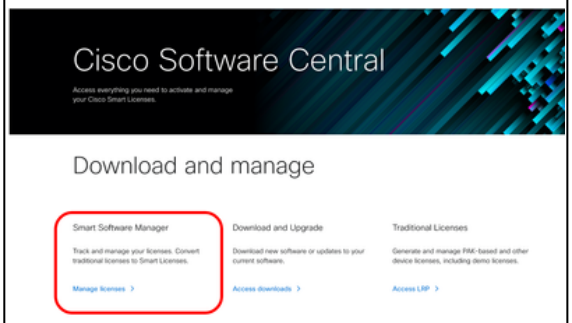
		Image - Servicekonfiguration der Management-Schnittstelle Schritt 18: Die AsyncOS-API (Überwachung) ist die neue Benutzeroberfläche des SWA. Wenn Sie die neuen Berichte für die Benutzeroberfläche verwenden möchten, legen Sie diese Option auf Y (Standard) fest. Andernfalls können Sie N eingeben und mit Schritt 20 fortfahren. Schritt 19: Sie können die standardmäßige neue GUI-HTTPS-Portnummer von 6443 in jede gewünschte Portnummer ändern, solange es keine Portkonflikte gibt. Drücken Sie die Eingabetaste, um den Standardport (TCP/6443) zu verwenden. Schritt 20: Die SWA-Verwaltungsschnittstelle verwendet das Cisco Demo-Zertifikat. Geben Sie Y ein, um das Demo-Zertifikat zu akzeptieren. Sie können das GUI-Zertifikat nach der Ersteinrichtung ändern. Schritt 21: Drücken Sie die Eingabetaste, um den ifconfig-Assistenten zu beenden.  Bild - Neue GUI-TCP-Konfiguration
	Standard-Gateway konfigurieren	Schritt 22: Führen Sie setgateway aus.

		Schritt 23: Wählen Sie IPv4 aus, wenn Ihre Verwaltungsschnittstelle mit IPv4 konfiguriert wurde, oder wählen Sie IPv6 aus. Schritt 24: Geben Sie die IP-Adresse des Standardgateways ein. Schritt 25: Speichern Sie die Änderungen, indem Sie commit ausführen. Schritt 26: (Optional) Sie können Notizen zu den gespeicherten Änderungen hinzufügen. Schritt 27: (Optional) Sie können SWA anweisen, die Konfiguration vor der Übernahme der Änderungen zu sichern.  Bild - Konfigurieren des Standard-Gateways
SSH	Traditionelle Lizenz importieren	 Hinweis: Wenn Sie Smart License verwenden, fahren Sie mit Schritt 36 fort.

		Schritt 28: Stellen Sie über SSH eine Verbindung mit SWA her. Schritt 29: Lizenz für Ladevorgang ausführen Schritt 30: Wählen Sie Einfügen über CLI aus. Schritt 31: Öffnen Sie Ihre Lizenzdatei mit einem Texteditor, und kopieren Sie den gesamten Inhalt. Schritt 32: Fügen Sie die Lizenz in die SSH-Shell ein. Schritt 33: Drücken Sie die Eingabetaste, um zu einem neuen Posten zu navigieren. Schritt 34: Halten Sie die Taste Steuerung gedrückt, und drücken Sie D. Schritt 35: Lesen Sie die Lizenzvereinbarung, und geben Sie YES ein, um die Bedingungen zu akzeptieren.  Bild - Import einer traditionellen Lizenz Fahren Sie mit Schritt 58 fort.
GUI	DNS-Server konfigurieren	Schritt 37: Melden Sie sich bei der GUI an (der Standardwert ist HTTPS://<SWA FQDN oder IP

		Address>:8443). Schritt 38: Navigieren Sie zu Netzwerk, und wählen Sie DNS aus. Schritt 39: Klicken Sie auf Einstellungen bearbeiten. Schritt 40: Wählen Sie im Abschnitt "Primary DNS Servers" (Primäre DNS-Server) die Option Use these DNS Servers (Diese DNS-Server verwenden) aus. Schritt 41: Setzen Sie die Priorität auf 0, und geben Sie die IP-Adresse Ihres DNS-Servers ein.  Hinweis: Sie können mehr als einen DNS-Server hinzufügen, indem Sie Zeile hinzufügen auswählen. Schritt 42: Senden. Schritt 43: Bestätigen Sie die Änderungen.

		 Image: Konfigurieren des DNS-Servers
	Smart License konfigurieren	Schritt 44: Wähle in der GUI von System Administration (Systemverwaltung) die Option Smart Software Licensing (Smart Software-Lizenzierung) aus. Schritt 45: Wähle EnableSmart Software Licensing (Smart-Softwarelizenzierung aktivieren).  Vorsicht: Sie können nicht von der Smart License zur Classic License zurückkehren, nachdem Sie die Smart License-Funktion auf Ihrer Appliance aktiviert haben. Schritt 46: Klicken Sie auf OK, um die Konfiguration der Smart License

		fortzusetzen. Schritt 47: Bestätigen Sie die Änderungen. Schritt 48: Melden Sie sich bei Cisco Software Central an, um das Token zur SWA-Registrierung zu erhalten (https://software.cisco.com/#) Schritt 49: Klicken Sie auf Lizenzen verwalten.  Bild - Cisco Smart License Management Schritt 50: Wählen Sie in Smart Software Licensing (Smart Software-Lizenzierung) Inventory (Bestand). Schritt 51: Erstellen Sie auf der Registerkarte Allgemein ein neues Token, oder verwenden Sie die verfügbaren Token.  Image - Smart Software-Lizenzinventarseite Schritt 52: Geben Sie die erforderlichen Informationen ein, und erstellen Sie ein Token.

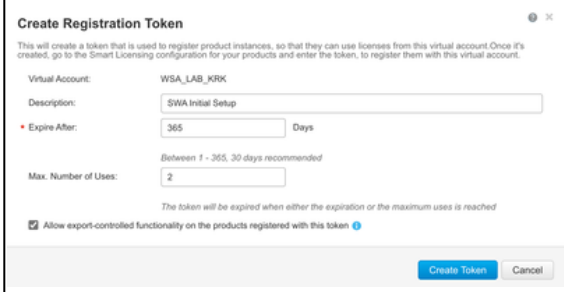
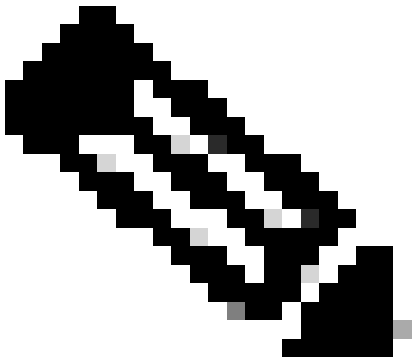


Bild - Erstellen eines Tokens

Schritt 53: Klicken Sie auf das blaue Symbol vor dem neu hinzugefügten Token, und kopieren Sie dessen Inhalt.

Bild: Kopieren des Tokens

Schritt 54: Navigieren Sie in der SWA-GUI zu Systemverwaltung, und wählen Sie Smart Software Licensing aus.



Hinweis: Wenn Sie sich bereits auf der Seite Smart Software Licensing befinden, aktualisieren Sie die Seite.

Schritt 55: (Optional) Wenn der SWA über keine Management-Schnittstelle auf das Internet zugreifen kann, können Sie die Test-Schnittstelle in die Schnittstellen ändern, die auf das Internet zugreifen dürfen.

Tipp: Weitere Informationen zu mehreren Schnittstellenkonfigurations- und Routing-Tabellen finden Sie im Abschnitt "Netzwerkkonfiguration" in diesem Artikel.

Schritt 56: Klicken Sie auf Registrieren.

Schritt 57: Fügen Sie das Token ein, und klicken Sie auf Registrieren.

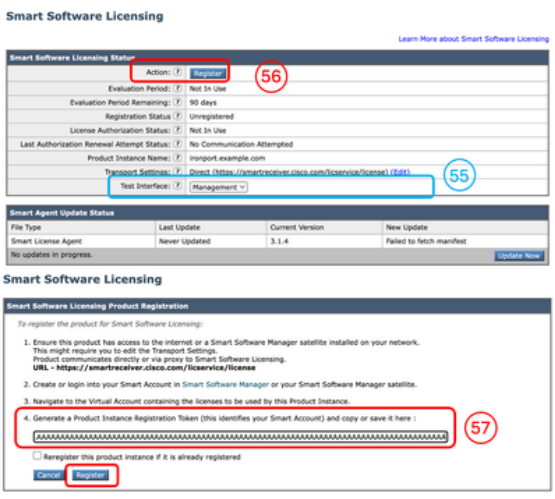
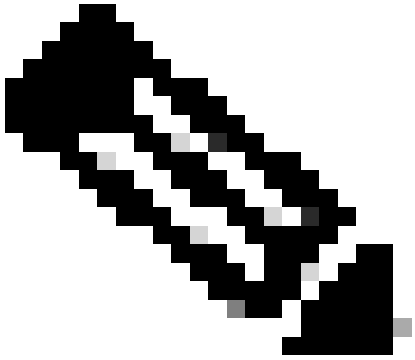
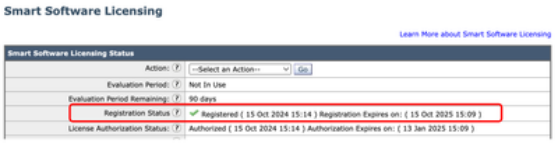


Bild: Registrierung von SWA für Smart License

		 Hinweis: Warten Sie einige Minuten, um Ihre Registrierung zu überprüfen, aktualisieren Sie die Smart Licensing-Seite in SWA, und überprüfen Sie den Registrierungsstatus.  Bild: Registrierungsstatus der Smart-Lizenz
	Systemeinrichtungs-Assistent	Schritt 58: Navigieren Sie in der SWA-GUI zu Systemverwaltung, und wählen Sie Systemeinrichtungsassistent aus. Schritt 59: Lesen und akzeptieren Sie die Bedingungen dieser Lizenzvereinbarung. Schritt 60: Klicken Sie auf Einrichtung starten. Schritt 61: Auswählen Standard aus dem Abschnitt "Betriebsmodus der Appliance". Schritt 62: Geben Sie den Standard-Systemhostnamen ein.

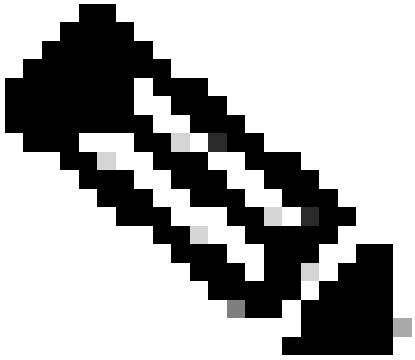
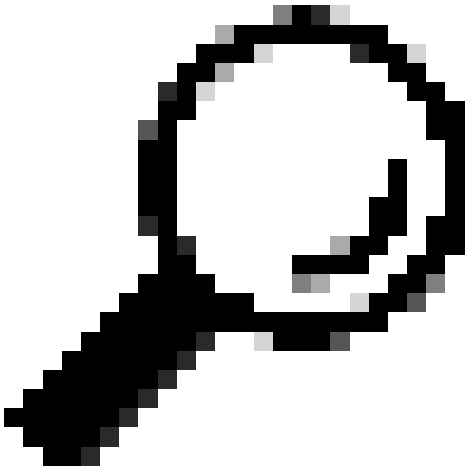
		 Hinweis: Der vorherige Hostname, der in Schritt 9 erstellt wurde, bezog sich auf die Verwaltungsschnittstelle und nicht auf den SWA.
		Schritt 63: Geben Sie die IP-Adresse des DNS-Servers bzw. der DNS-Server ein. Schritt 64: Sie können den NTP-Server (Network Time Protocol) konfigurieren.
		 Tipp: Wenn Ihr NTP-Server Authentifizierung erfordert, können Sie die Schlüsselparameter konfigurieren.
		Schritt 65: Wählen Sie die Zeitzone aus, die für das SWA gilt, und klicken Sie auf Weiter.

Bild - Systemeinrichtungsassistent - Systemeinstellungen

Schritt 66. (Optional) Wenn Sie einen Upstream-Proxy in Ihrem Netzwerk verwenden, können Sie diesen auf der Seite Netzwerkkontext konfigurieren oder als Standard beibehalten, und klicken Sie auf Weiter.

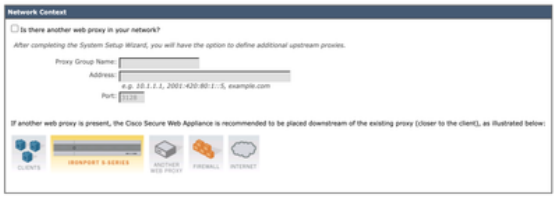
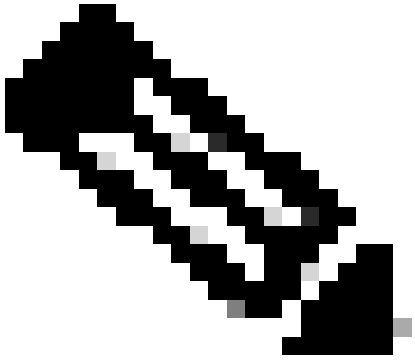
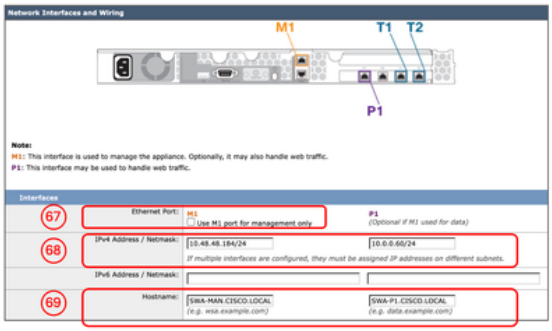


Bild - Systemeinrichtungsassistent - Upstream-Proxykonfiguration

Schritt 67: (Optional) Wenn Sie den Datenverkehr der Management-Schnittstelle vom Datenverkehr der Datenschnittstellen (P1- und P2-Schnittstellen) trennen müssen, wählen Sie M1-Port nur für Management verwenden aus.

Schritt 68. (Optional) Sie können die IP-Adresse der Netzwerkschnittstellen aus dem Abschnitt "IPv4-Adresse/Netzmaske" oder "IPv6-Adresse/Netzmaske" hinzufügen oder ändern.

Schritt 69. (Optional) Sie können den Netzwerkschnittstellen-Hostnamen hinzufügen oder ändern, und klicken Sie auf "Weiter".

		 Hinweis: Der P1-Port kann über den Systemeinrichtungsassistenten aktiviert und konfiguriert werden. Wenn Sie die P2-Schnittstelle aktivieren möchten, müssen Sie dies nach Abschluss des Assistenten für die Systemeinrichtung tun.  Abbild - Systemeinrichtungsassistent - Konfiguration der Netzwerkschnittstellen Schritt 70. (Optional) Falls Sie die Layer 4-Datenverkehrsüberwachung (L4TM) konfigurieren möchten, können Sie die Duplex-Einstellung konfigurieren. Andernfalls können Sie die Standardeinstellung beibehalten und auf "Weiter" klicken.

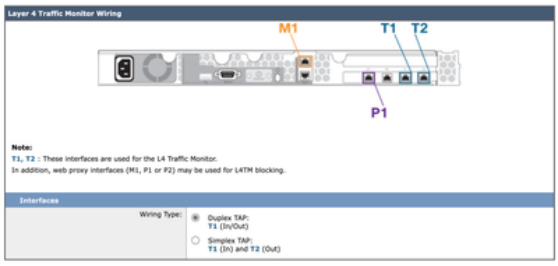
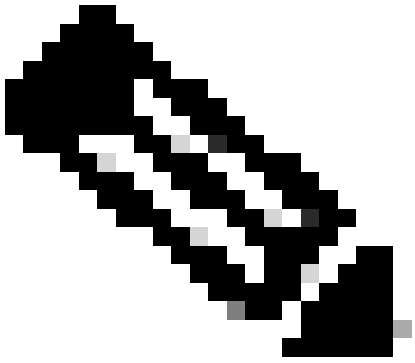


Bild - Systemeinrichtungsassistent - Einstellung der Layer-4-Datenverkehrsüberwachung

Schritt 71. (Optional) Auf der Seite IPv4 Routes for Management können Sie das Standard-Gateway ändern.

Schritt 72: (Optional) Sie können eine Route hinzufügen, um statische Routen zu erstellen.



Hinweis: Wenn Sie in Schritt 67 "M1-Port nur für Management verwenden" wählen, gibt es zwei separate Routing-Tabellen für die Management-Schnittstelle und die Datenschnittstellen (P1 und P2).

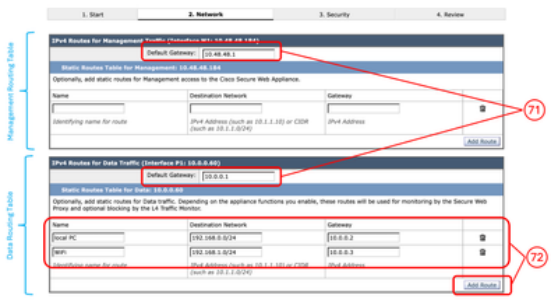
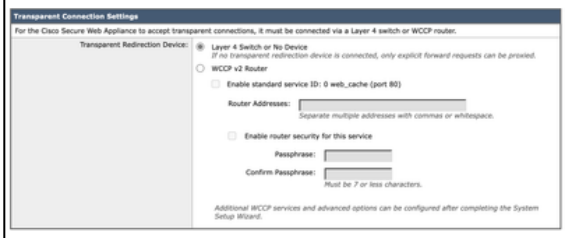


		Bild - Systemeinrichtungsassistent - Route hinzufügen Schritt 73: (Optional) Wenn Sie die Bereitstellung von Transparent Proxy über das Web Cache Communication Protocol (WCCP) einrichten möchten, können Sie die WCCP-Einstellungen konfigurieren. Andernfalls können Sie den Standard-Layer-4-Switch oder "Kein Gerät" belassen und auf Weiter klicken.  Bild - Systemeinrichtungsassistent - Proxy-Bereitstellungskonfiguration Schritt 74: Richten Sie ein neues Kennwort für das Administratorkonto ein. Schritt 75: Geben Sie eine E-Mail-Adresse ein, die voraussichtlich Systemwarnungen erhalten wird. Schritt 76: (Optional) Geben Sie die SMTP-Relay-Hostinformationen (Simple Mail Transfer Protocol) an, andernfalls lassen Sie das Feld leer. Wenn kein interner Relay-Host definiert ist, verwendet SMTP die DNS-Suche des MX-Datensatzes. Schritt 77. (Optional) Wenn Sie die Teilnahme am Cisco SensorBase-Netzwerk deaktivieren möchten, deaktivieren Sie das Kontrollkästchen Netzwerkteilnahme, oder belassen Sie die Standardeinstellung, und klicken Sie auf Weiter.

Hinweis: Die Teilnahme am Cisco SensorBase-Netzwerk bedeutet, dass Cisco Daten sammelt und diese an die SensorBase-Datenbank für Bedrohungsmanagement weitergibt.

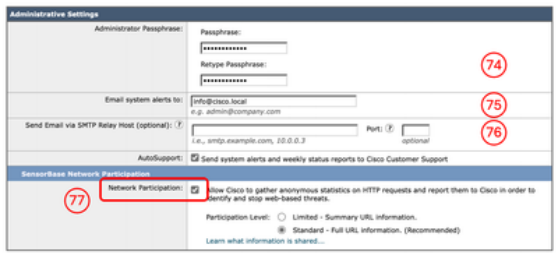


Bild - Systemeinrichtungsassistent - Verwaltungseinstellungen

Schritt 78. (Optional) Sie können die Standardaktionen für Globale Richtlinie, L4TM und Cisco Data Security Filtering ändern. Sie können die Standardaktionen auch beibehalten und auf "Weiter" klicken.

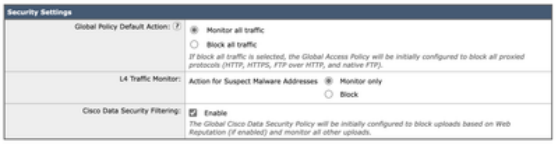


Bild - Systemeinrichtungsassistent - Sicherheitseinstellungen

Schritt 79: Überprüfen Sie Ihre Konfiguration. Wenn Sie Änderungen vornehmen müssen, klicken Sie auf die Schaltfläche "Zurück", um zur

		vorherigen Seite zurückzukehren, oder klicken Sie auf "Diese Konfiguration installieren".

Netzwerkkonfiguration

Zum Konfigurieren der Netzwerkschnittstelle können Sie sowohl die CLI als auch die GUI verwenden.

	Befehl/Pfad	Aktion
Konfigurieren von Netzwerkschnittstellenkarten über CLI	CLI > ifconfig	Neu: Wenn die Schnittstelle nicht in der Ausgabe von ifconfig aufgeführt ist, sondern auf der virtuellen Maschine oder der physischen Appliance vorhanden ist, können Sie mit diesem Befehl die Schnittstelle in der Liste anzeigen. Bearbeiten: Mit dieser Aktion können Sie die IP-Adresse, die Subnetzmaske, den Schnittstellen-Hostnamen oder andere verwandte Parameter bearbeiten. Details: Zeigt Details einer Schnittstelle an, wie MAC-Adresse, Medientyp, Duplexmodus usw. Delete (Löschen): Entfernt die Schnittstelle aus der Liste ifconfig und entfernt die IP-Adresse, wenn sie zuvor zugewiesen wurde.
Konfigurieren von Netzwerkschnittstellenkarten über die Benutzeroberfläche	GUI > Netzwerk > Schnittstellen	Sie können die IP-Adresse und den Hostnamen der Schnittstelle bearbeiten. Sie können die Portnummer des

		Appliance-Verwaltungsdienste wie FTP, SSH, HTTP-Zugriff und HTTPS-Zugriff.

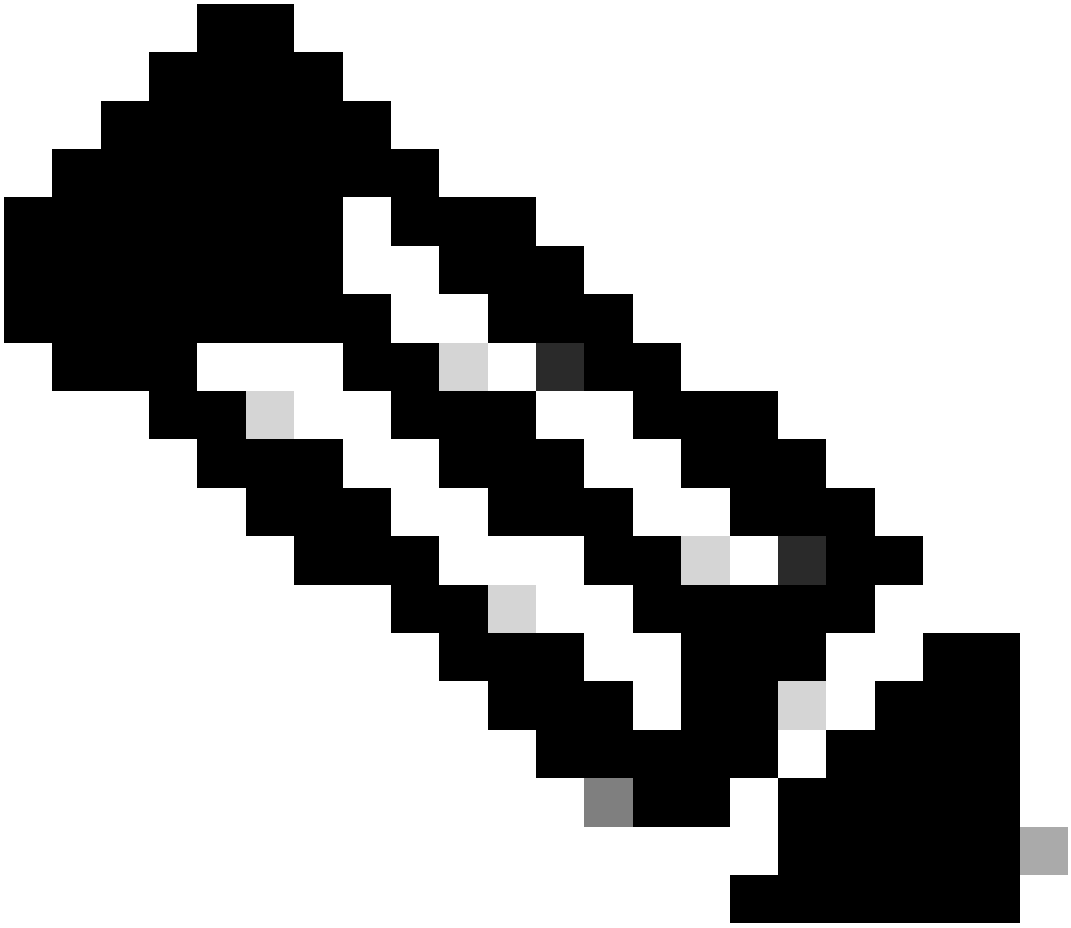
Routingtabelle

Routen sind wichtig, um zu bestimmen, wohin der Netzwerkverkehr geleitet werden soll. Das SWA verarbeitet diese Arten von Datenverkehr:

- Datenverkehr: Dies umfasst den vom Webproxy verarbeiteten Datenverkehr von Endbenutzern, die im Internet surfen.
- Management-Datenverkehr: Dies umfasst Datenverkehr, der durch das Management der Appliance über die Webschnittstelle generiert wird, sowie Datenverkehr für Management-Services wie SWA-Upgrades, Komponenten-Updates, DNS, Authentifizierung und andere damit verbundene Aufgaben.

Standardmäßig verwenden beide Datenverkehrstypen die für alle konfigurierten Netzwerkschnittstellen definierten Routen. Sie haben jedoch die Möglichkeit, das Routing zu trennen, sodass der Verwaltungsverkehr eine dedizierte Management-Routing-Tabelle und der Datenverkehr eine separate Daten-Routing-Tabelle verwendet.

Verwaltungsdatenverkehr	Datenverkehr
WebUI SSH SNMP Authentifizierung, mit Domain Controller (konfigurierbar) Syslogs FTP-Push DNS (konfigurierbar) Update/Upgrade/Feature-Schlüssel (konfigurierbar)	HTTP-Proxy HTTPS-Proxy FTP-Proxy WCCP-Verhandlung ICAP-Anforderung mit externem SvD-Server DNS (konfigurierbar) Update/Upgrade/Feature-Schlüssel (konfigurierbar) Authentifizierung mit Domänencontroller (konfigurierbar)



Hinweis: Wenn Sie die Option "M1-Port nur für Management verwenden" auswählen, wird dem SWA eine zusätzliche Routing-Tabelle hinzugefügt, die als Data Routing-Tabelle bezeichnet wird. Diese Routing-Tabelle enthält nur ein konfigurierbares Standard-Gateway. Alle zusätzlichen Routing-Pfade müssen manuell konfiguriert werden.

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance
- Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco
- Best Practices für sichere Web-Appliances
- Firewall für sichere Web-Appliance konfigurieren
- Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren

- SNMP in SWA konfigurieren und Fehlerbehebung dafür durchführen
- Konfigurieren von SCP-Push-Protokollen in der sicheren Web-Appliance mit Microsoft Server
- Aktivierung bestimmter YouTube-Kanäle/Videos und Blockierung sonstiger YouTube-Inhalte in SWA
- HTTPS-Zugriffsformat in sicherer Web-Appliance
- Zugreifen auf Protokolle der sicheren Web-Appliance
- Umgehen der Authentifizierung in einer sicheren Web-Appliance
- Blockieren von Datenverkehr in einer sicheren Web-Appliance
- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.