Secure Web Appliance 초기 설정 구성

목차

소개

이 문서에서는 SWA(Secure Web Appliance)를 처음 구성하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.
- 기본 네트워킹 원칙.

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.
- SWA GUI(Graphical User Interface)에 대한 관리 액세스
- SWA CLI(Command Line Interface)에 대한 관리 액세스
- SWA 콘솔에 대한 관리 액세스.
- 유효한 SWA 라이센스 또는 Smart License Management 포털에 대한 액세스(Smart 라이센스를 사용 중인 경우).

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

SWA 설치

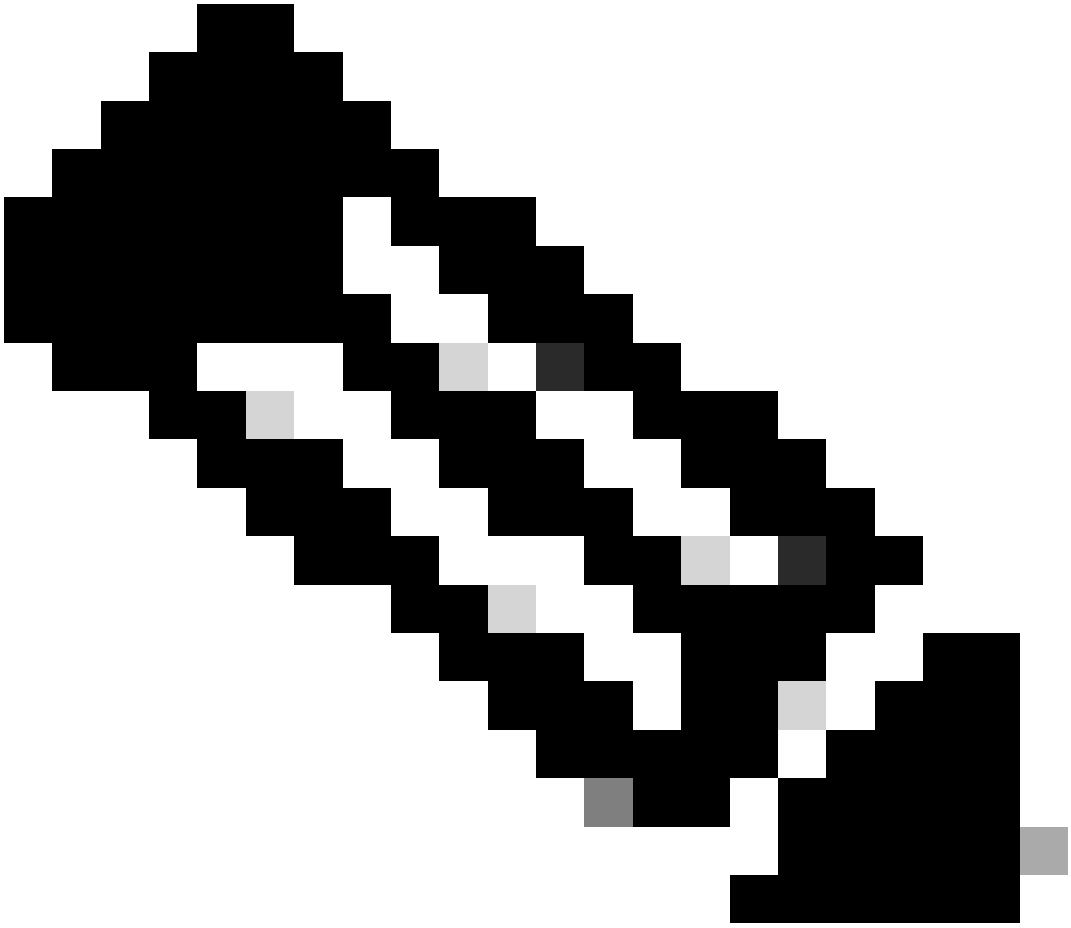
Cisco SWA는 조직의 웹 보안 및 제어를 강화하도록 설계된 전달 프록시 솔루션입니다. 가상 및 물리적 양식으로 제공되는 SWA는 다양한 요구를 충족할 수 있는 유연한 구축 옵션을 제공합니다. 가상 SWA는 Microsoft Hyper-V, VMware ESX 및 KVM을 비롯한 여러 하이퍼바이저 플랫폼을 지원하여 다양한 가상 환경과의 호환성을 보장합니다. 물리적 어플라이언스를 선호하는 고객을 위해 Cisco는 S100, S300, S600이라는 세 가지 다른 모델을 제공합니다. 각 모델은 다양한 수준의 성능 및 용량 요구 사항을 충족하도록 설계되어 조직이 특정 웹 보안 요구 사항에 적합한 솔루션을 찾을 수 있도록 보장합니다.

가상 머신 이미지를 다운로드하려면 https://software.cisco.com/download/home을 방문하십시오. 를 참조하십시오.

가상 Cisco SWA를 설치하는 것은 적절한 하이퍼바이저 플랫폼을 선택하는 것부터 시작되는 간단한 프로세스입니다. 먼저 Cisco 웹 사이트에서 가상 SWA 설치 파일을 다운로드합니다. VMware ESX의 경우 OVA 파일을 구축하여 네트워크 설정을 구성하고 CPU, 메모리 및 스토리지와 같은 충분한 리소스를 할당합니다. Microsoft Hyper-V의 경우 다운로드한 VHD 파일을 Hyper-V 관리자로 가져오고 그에 따라 가상 컴퓨터 설정을 구성합니다. KVM의 경우 virt-manager 또는 virsh 명령줄 도구를 사용하여 다운로드한 이미지를 사용하여 가상 머신을 정의하고 시작합니다. 가상 머신이 작동 및 실행되면 이 문서의 단계를 사용하여 초기 설정을 수행할 수 있습니다.

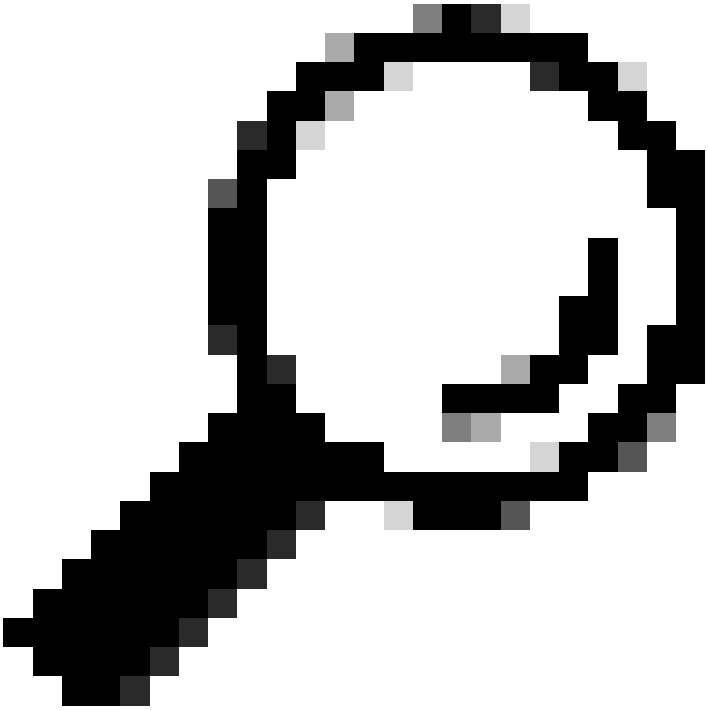
초기 설정

SWA를 설치한 후 초기 구축을 위해 다음 단계를 진행합니다.

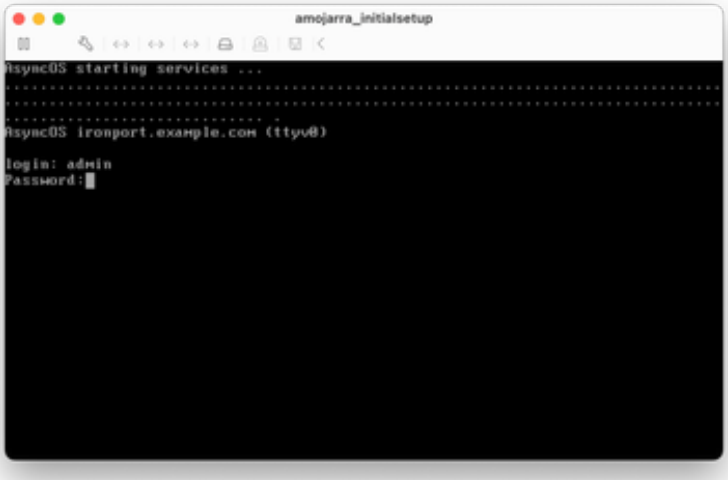


참고: 초기 설정에서는 콘솔, SSH 및 GUI를 통해 SWA에 액세스해야 합니다.

연결 방법	단계	컨피그레이션 단계
Console	IP 주소 구성	1단계. CLI에 로그인하려면 사용자 이름 및 비밀번호를 입력합니다.



팁: 기본 사용자 이름은 admin이고 기본 비밀번호는 ironport입니다.



이미지 - 로그인 화면

2단계. ifconfig를 실행합니다.

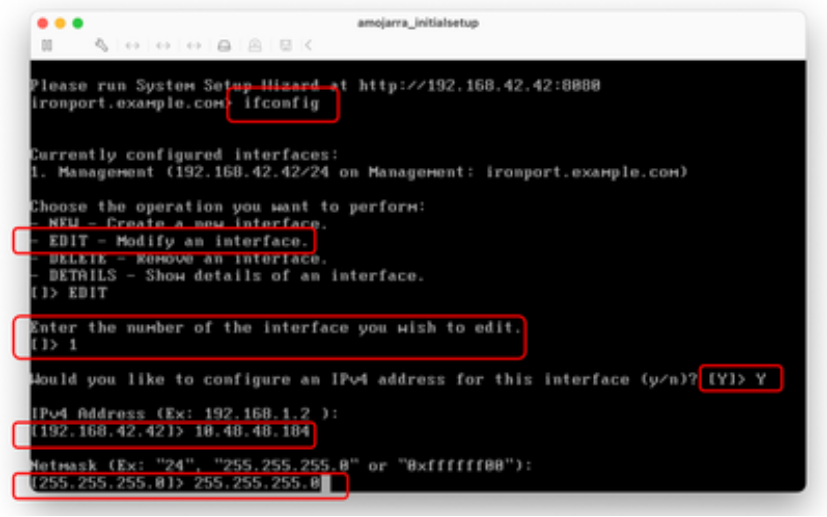
3단계. 편집을 선택합니다.

4단계. 관리 인터페이스와 연결된 번호를 입력합니다.

5단계. 기본 IPv4 주소를 편집하려면 Y를 선택합니다.

6단계. IP 주소를 입력합니다

7단계. 서브넷 마스크를 입력합니다.



이미지 - 관리 인터페이스 IP 주소 편집

8단계. IPv6를 구성하려면 "IPv6를 구성하시겠습니까?"라는 질문에 Y를 입력하고, 그렇지 않으면 이 값을 기본값(No)으로 두고 Enter를 누릅니다.

9단계. 호스트 이름으로 FQDN(정규화된 도메인 이름)을 입력합니다.

10단계. 관리 인터페이스에 대한 FTP(File Transfer Protocol) 액세스를 활성화하려면 Y를 선택하거나 Enter 키를 누릅니다.

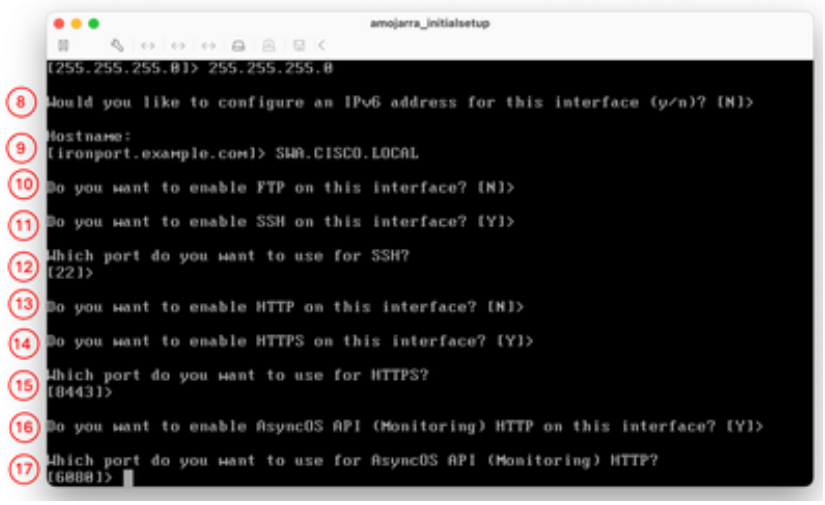
11단계. SSH(Secure Shell)는 기본적으로 사용으로 설정되어 있습니다. SSH를 사용하도록 설정하는 것이 좋습니다. 계속하려면 Y를 입력합니다.

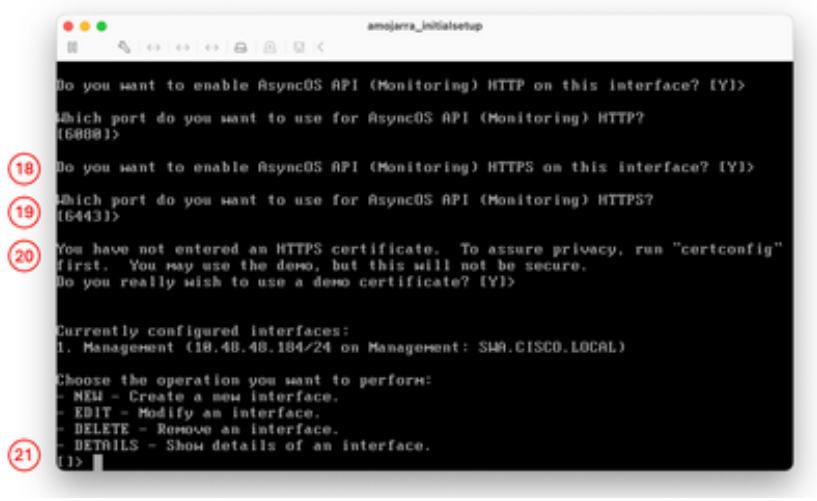
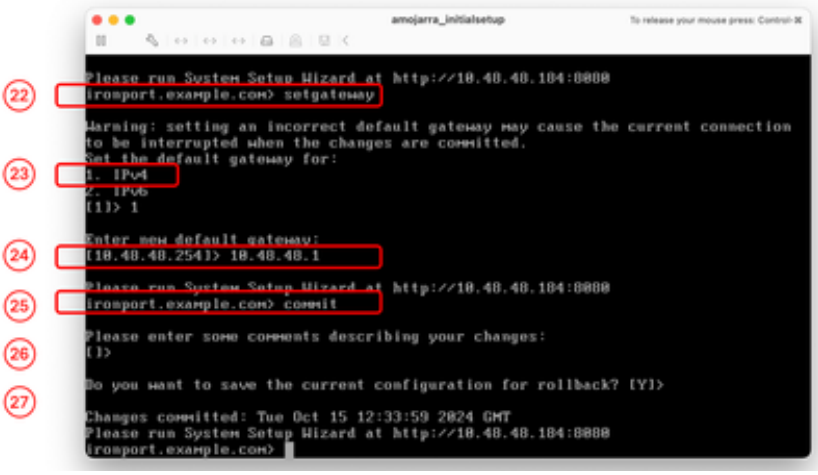
12단계(선택 사항) 기본 SSH 포트를 TCP 22에서 원하는 포트 번호로 변경할 수 있습니다. 다른 포트 충돌이 없으면 Enter를 눌러 기본 포트(TCP/22)를 사용합니다.

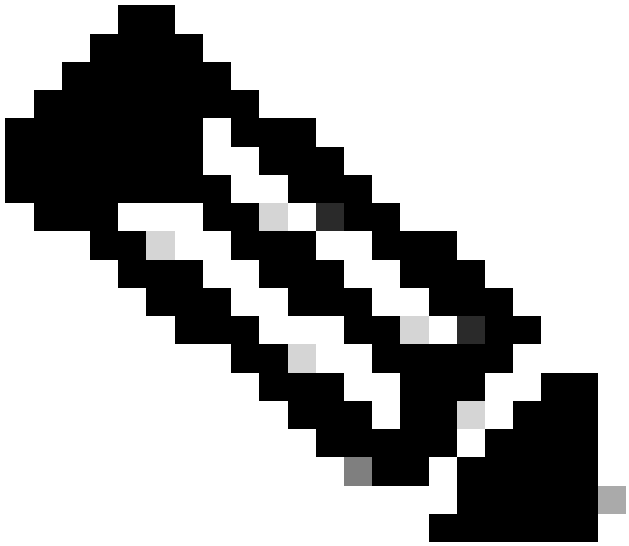
13단계. 관리 인터페이스에 HTTP(Hypertext Transfer Protocol) 액세스를 허용하려면 Y를 입력하고 HTTP 액세스용 포트 번호를 설정합니다. 그렇지 않으면 관리 인터페이스에 대한 HTTPS(Hypertext Transfer Protocol Secure) 액세스만 갖도록 N을 선택할 수 있습니다.

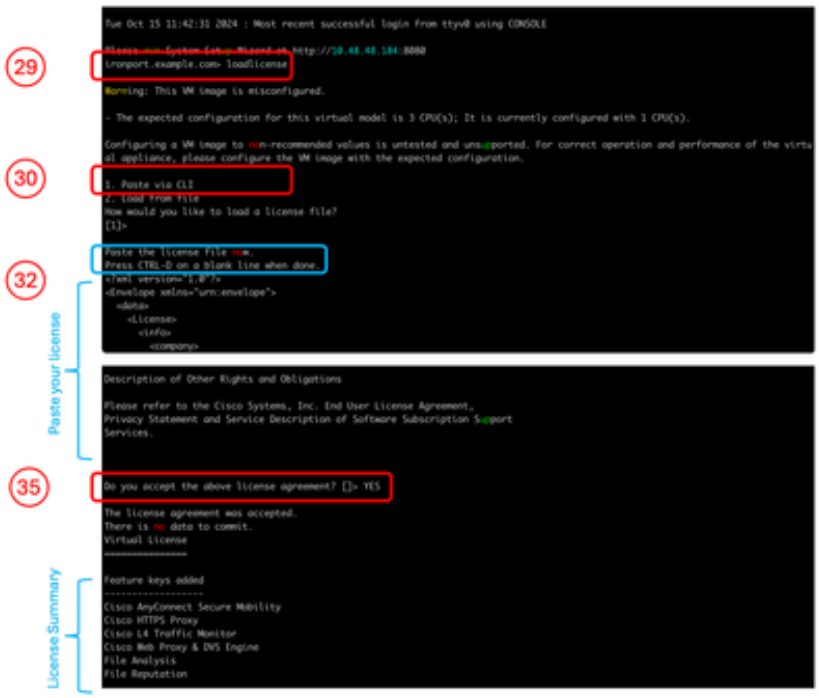
14단계. Y를 입력하고 Enter를 눌러 관리 인터페이스에 대한 HTTPS 액세스를 활성화합니다.

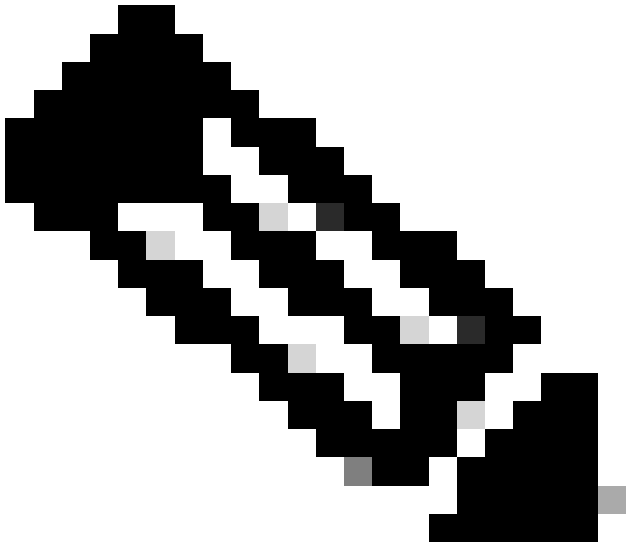
15단계. 기본 HTTPS 포트 번호를 8443에서 원하는 임의의 포트 번호로 변경할 수 있습니다. 단, 포트 충돌이 없는 경우에는 Enter 키를 눌러 기본 포트(TCP/8443)를 사용합니

		다. 16단계. API(Application Programming Interface)는 기본적으로 Enable(활성화)로 설정되어 있습니다. API를 사용하지 않는 경우 N을 입력하고 Enter 키를 눌러 API를 비활성화할 수 있습니다. 17단계. API를 활성화하도록 선택한 경우 기본 API 포트 번호를 6080에서 원하는 포트 번호로 변경할 수 있습니다. 단, 포트 충돌이 없는 경우에는 Enter 키를 눌러 기본 포트(TCP/6080)를 사용합니다.  이미지 - 관리 인터페이스 서비스 컨피그레이션 18단계. AsyncOS API(모니터링)는 SWA의 새 GUI입니다. 새 사용자 인터페이스 보고서를 사용하려면 이 옵션을 Y(기본값)로 설정하고, 그렇지 않으면 N을 입력하고 20단계로 건너뛸 수 있습니다 19단계. 기본 New GUI HTTPS 포트 번호를 6443에서 원하는 포트 번호로 변경할 수 있습니다. 단, 포트 충돌이 없는 경우에는 Enter 키를 눌러 기본 포트(TCP/6443)를 사용합니다. 20단계. SWA 관리 인터페이스는 Cisco 데모 인증서를 사용합니다. 데모 인증서를 수락하려면 Y를 입력합니다. 초기 설정 후 GUI 인증서를 변경할 수 있습니다. 21단계. Enter 키를 눌러 ifconfig 마법사를 종료합니다.

		 이미지 - 새 GUI TCP 컨피그레이션
기본 게이트웨이 구성	22단계. setgateway를 실행합니다. 23단계. 관리 인터페이스가 IPv4로 구성된 경우 IPv4를 선택하거나 IPv6을 선택합니다. 24단계. 기본 게이트웨이 IP 주소를 입력합니다. 25단계. commit을 실행하여 변경 사항을 저장합니다. 26단계(선택 사항) 저장 중인 변경 사항에 대한 메모를 추가할 수 있습니다 27단계(선택 사항) SWA를 사용하여 변경 사항을 적용하기 전에 컨피그레이션을 백업할 수 있습니다.	 이미지 - 기본 게이트웨이 구성

SSH	기존 라이센스 가져오기	 참고: Smart License를 사용하는 경우 36단계로 건너뜁니다. 28단계. SSH를 통해 SWA에 연결합니다. 29단계. loadlicense 실행 30단계. Paste via CLI(CLI를 통해 붙여넣기)를 선택합니다. 31단계. 텍스트 편집기로 라이센스 파일을 열고 모든 내용을 복사합니다. 32단계. SSH 셸에 라이센스를 붙여넣습니다. 33단계. Enter를 눌러 새 라인으로 이동합니다. 34단계. Ctrl을 누르고 D 키를 누릅니다. 35단계. 라이센스 계약서를 읽고 YES를 입력하여 조건에 동의합니다.

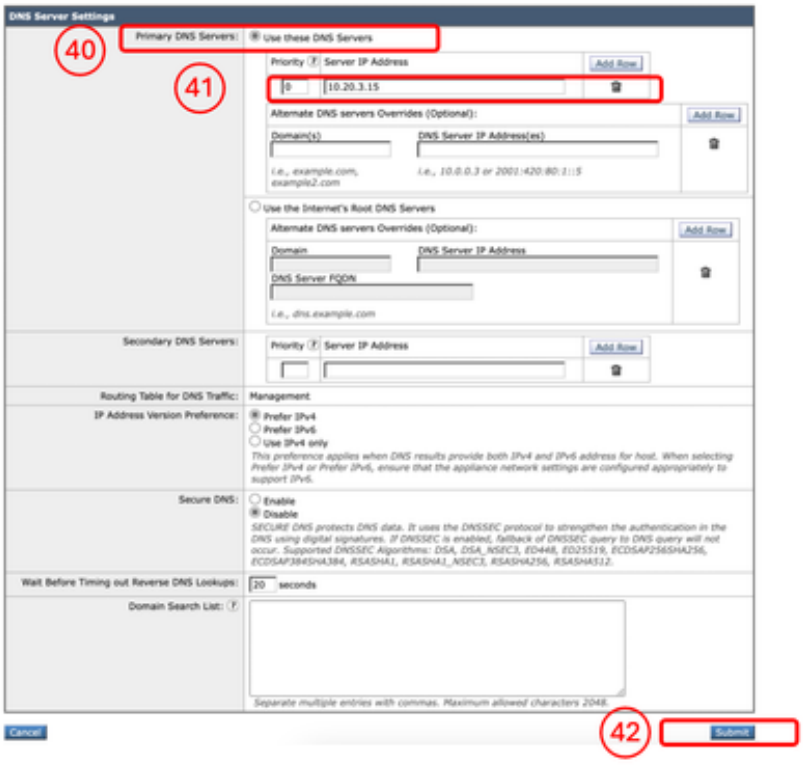
		 이미지 - 기존 라이센스 가져오기 58단계로 건너뜁니다.
GUI	DNS 서버 구성	37단계. GUI에 로그인합니다(기본값은 HTTPS://<SWA FQDN 또는 IP Address>:8443). 38단계. Network(네트워크)로 이동하고 DNS(DNS)를 선택합니다. 39단계. Edit Settings(설정 편집)를 클릭합니다. 40단계. Primary DNS Servers(기본 DNS 서버) 섹션에서 Use these DNS Servers(이 DNS 서버 사용)를 선택합니다. 41단계. Priority(우선순위)를 0으로 설정하고 DNS 서버 IP 주소를 입력합니다.



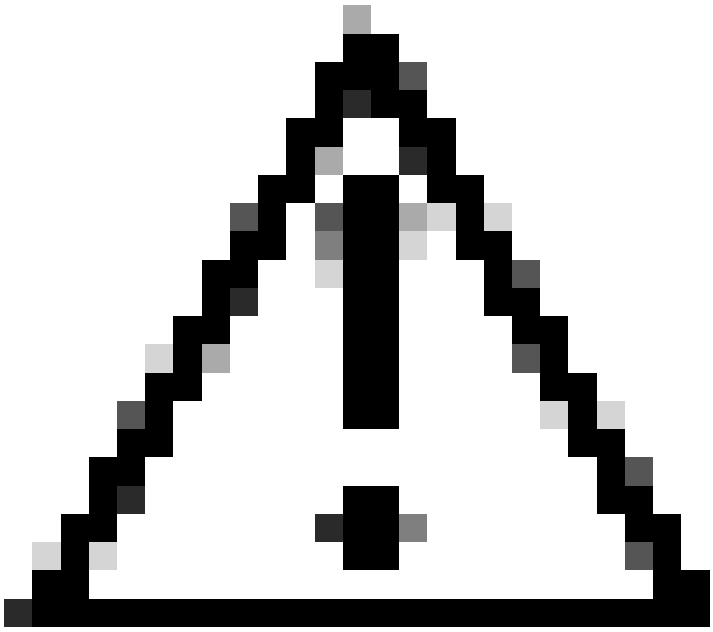
참고: Add Row(행 추가)를 선택하여 둘 이상의 DNS 서버를 추가할 수 있습니다.

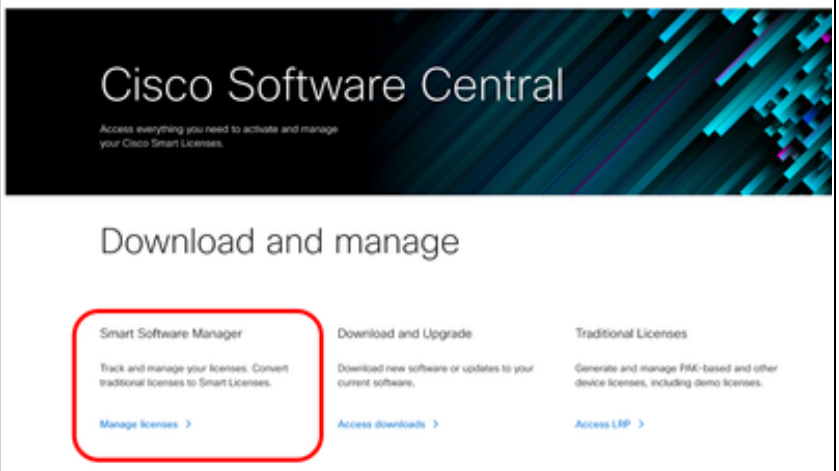
42단계. 제출합니다.

43단계. 변경 사항을 커밋합니다.



이미지 - DNS 서버 구성

	Smart 라이센스 구성	44단계. System Administration(시스템 관리)의 GUI에서 Smart Software Licensing(스마트 소프트웨어 라이센싱)을 선택합니다. 45단계. EnableSmart Software Licensing을 선택합니다.  주의: 어플라이언스에서 Smart License 기능을 활성화한 후에는 Smart License에서 Classic License로 롤백할 수 없습니다. 46단계. OK(확인)를 클릭하여 Smart License 구성을 계속합니다. 47단계. 변경 사항을 커밋합니다. 48단계. SWA를 등록할 토큰을 얻으려면 Cisco Software Central(https://software.cisco.com/#)에 로그인합니다 49단계. Manage Licenses(라이센스 관리)를 클릭합니다.



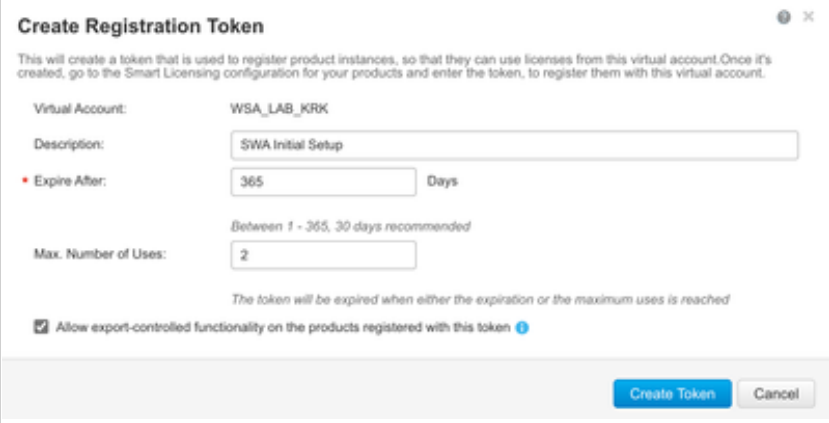
이미지 - Cisco Smart License 관리

50단계. Smart Software Licensing에서 Inventory(인벤토리)를 선택합니다.

51단계. General(일반) 탭에서 Create a New Token(새 토큰 생성) 또는 사용 가능한 토큰을 사용합니다.

이미지 - Smart Software License 인벤토리 페이지

52단계. 필수 정보를 입력하고 토큰 생성을 클릭합니다.

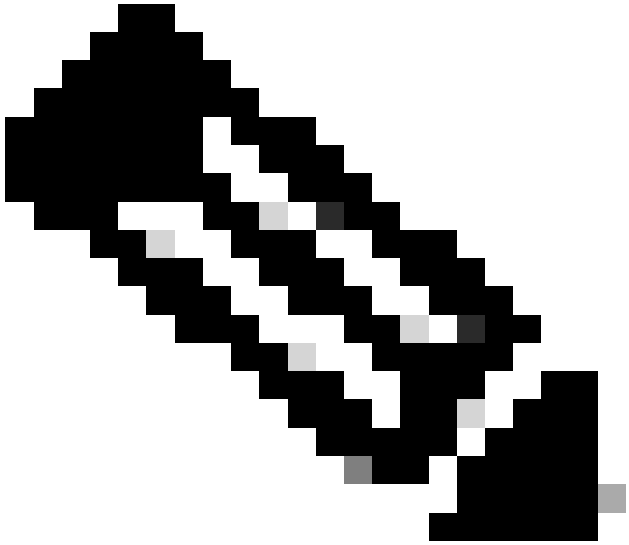


이미지 - 토큰 생성

53단계. 새로 추가된 토큰 앞의 파란색 아이콘을 클릭하고 내용을 복사합니다.

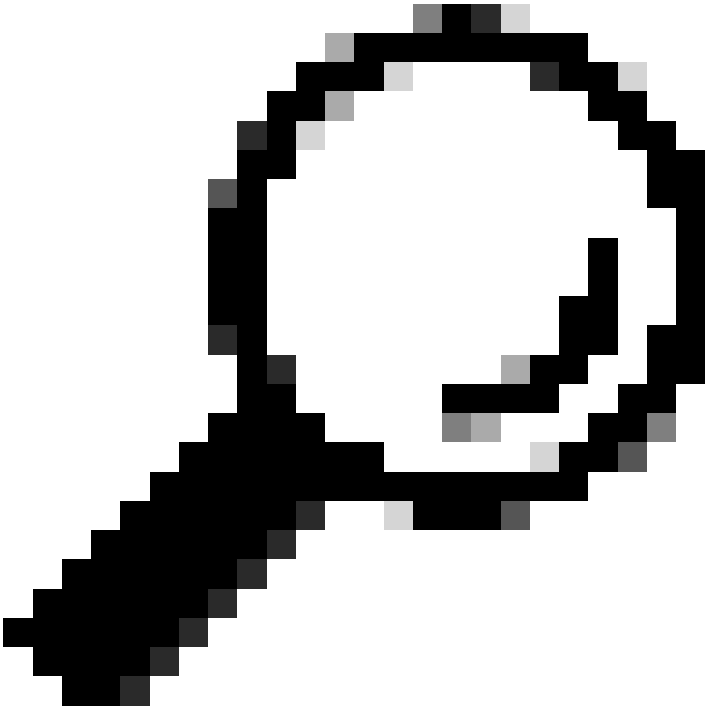
이미지 - 토큰 복사

54단계. SWA GUI에서 System Administration(시스템 관리)으로 이동하고 Smart Software Licensing(스마트 소프트웨어 라이센싱)을 선택합니다.



참고: 이미 Smart Software Licensing(Smart Software 라이센스) 페이지에 있는 경우 페이지를 새로 고치십시오.

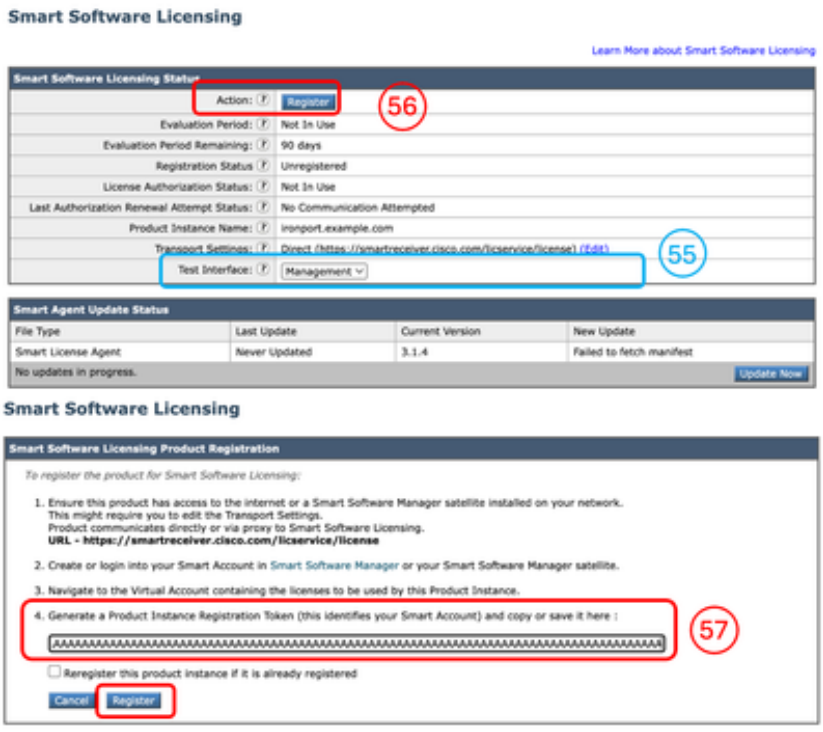
55단계(선택 사항) SWA가 관리 인터페이스에서 인터넷에 액세스할 수 없는 경우 테스트 인터페이스를 인터넷 액세스가 허용되는 인터페이스로 변경할 수 있습니다.

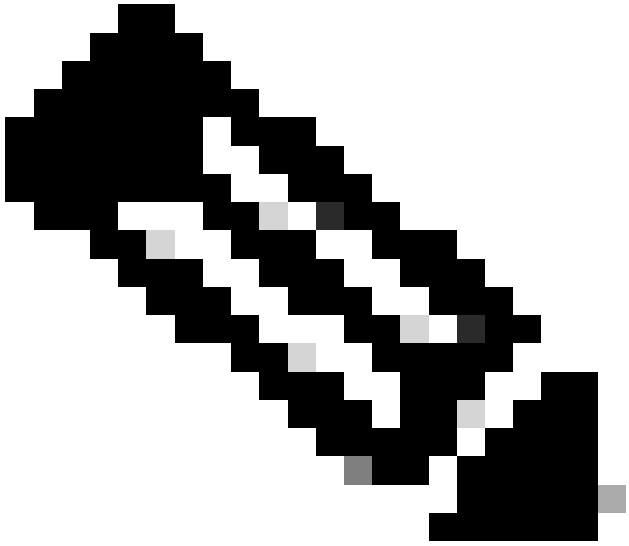
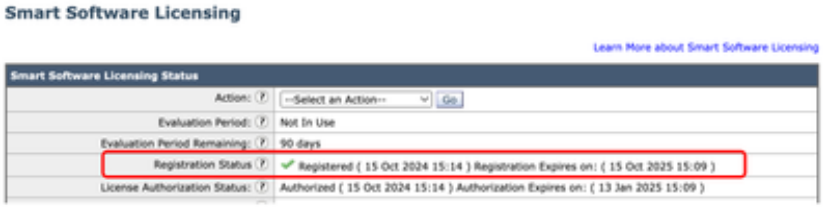


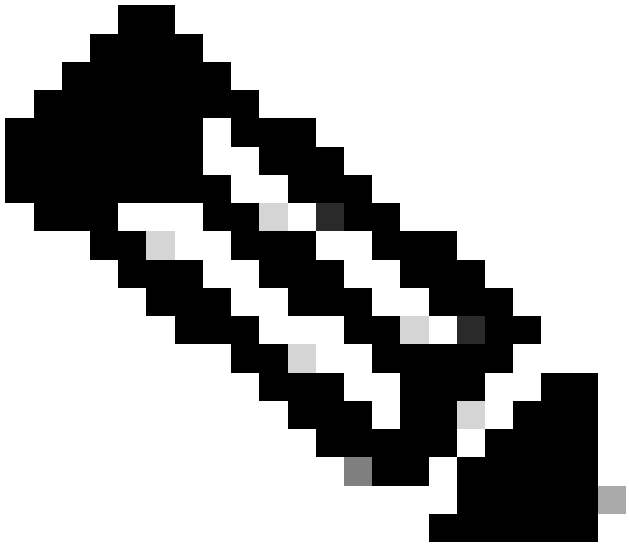
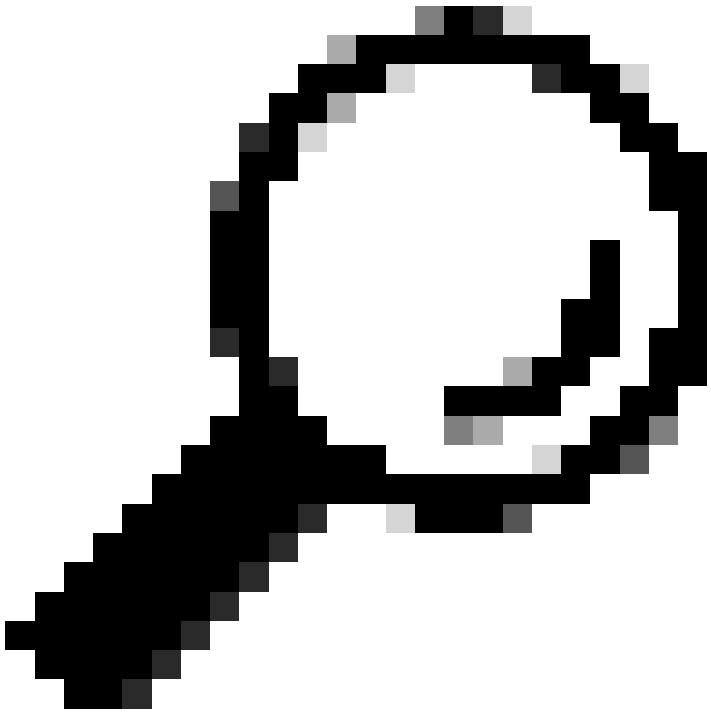
팁: 여러 인터페이스 컨피그레이션 및 라우팅 테이블에 대한 자세한 내용은 이 문서의 네트워크 컨피그레이션 섹션을 참조하십시오.

56단계. Register(등록)를 클릭합니다.

57단계. Token(토큰)을 붙여넣고 Register(등록)를 클릭합니다.



		이미지 - Smart License에 SWA 등록  참고: 등록을 확인하려면 몇 분 정도 기다렸다가 SWA에서 Smart Licensing 페이지를 새로 고치고 등록 상태를 확인합니다.  이미지 - Smart License 등록 상태
	시스템 설정 마법사	58단계. SWA GUI에서 System Administration(시스템 관리)으로 이동하고 System Setup Wizard(시스템 설정 마법사)를 선택합니다. 59단계. 이 사용권 계약 내용을 읽고 동의합니다. 60단계. Begin Setup(설정 시작)을 클릭합니다. 61단계. 선택 표준: Appliance Mode of Operation(어플라이언스 작동 모드) 섹션. 62단계. 기본 시스템 호스트 이름을 입력합니다.

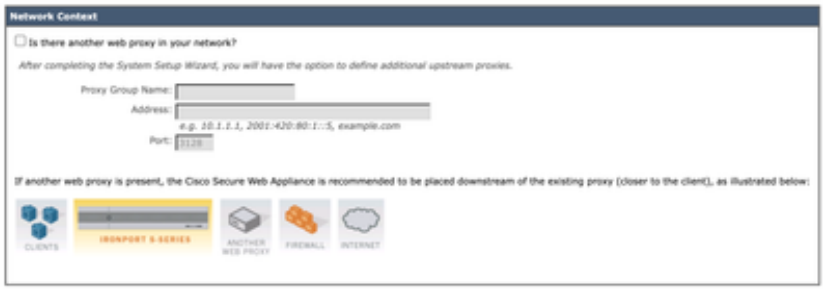
		 참고: 9단계에서 생성된 이전 호스트 이름은 SWA가 아니라 관리 인터페이스와 관련된 것이었습니다. 63단계. DNS 서버 IP 주소를 입력합니다. 64단계. NTP(Network Time Protocol) 서버를 구성할 수 있습니다.  팁: NTP 서버에 인증이 필요한 경우 Key 매개변수

를 구성할 수 있습니다.

65단계. SWA에 적용되는 표준 시간대를 선택하고 Next(다음)를 클릭합니다.

이미지 - 시스템 설정 마법사 - 시스템 설정

66단계(선택 사항) 네트워크에서 업스트림 프록시를 사용 중인 경우 Network Context(네트워크 컨텍스트) 페이지에서 구성하거나 기본값으로 유지하고 Next(다음)를 클릭합니다.



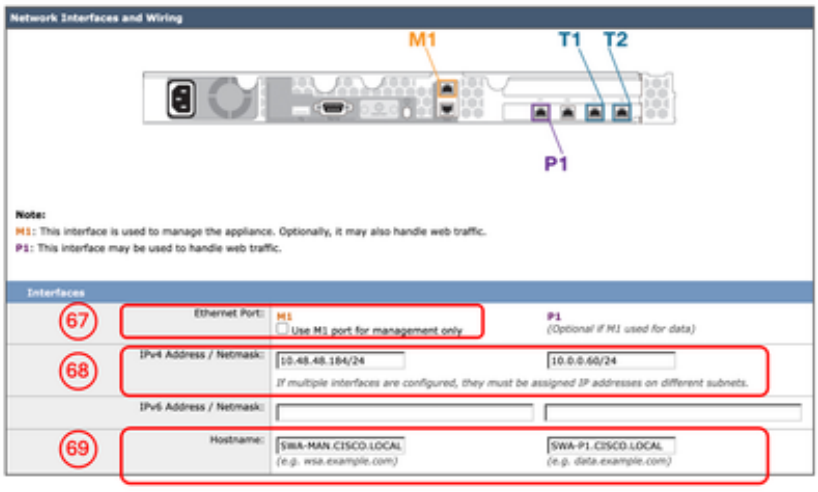
이미지 - 시스템 설정 마법사 - 업스트림 프록시 컨피그레이션

67단계(선택 사항) 관리 인터페이스 트래픽을 데이터 인터페이스(P1 및 P2 인터페이스) 트래픽과 분리해야 하는 경우 Use M1 port for management only를 선택합니다.

68단계(선택 사항) IPv4 Address/Netmask 또는 IPv6 Address/Netmask 섹션에서 네트워크 인터페이스 IP 주소를 추가하거나 수정할 수 있습니다.

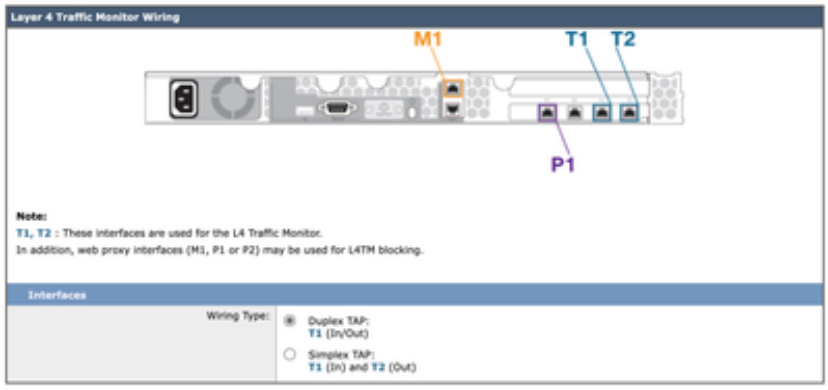
69단계(선택 사항) Network Interfaces Hostname(네트워크 인터페이스 호스트 이름)을 추가하거나 수정하고 Next(다음)를 클릭할 수 있습니다.

참고: P1 포트는 시스템 설정 마법사를 통해 활성화 및 구성할 수 있습니다. P2 인터페이스를 활성화하려면 시스템 설정 마법사를 완료한 후 이 작업을 수행해야 합니다.



이미지 - 시스템 설정 마법사 - 네트워크 인터페이스 컨피그레이션

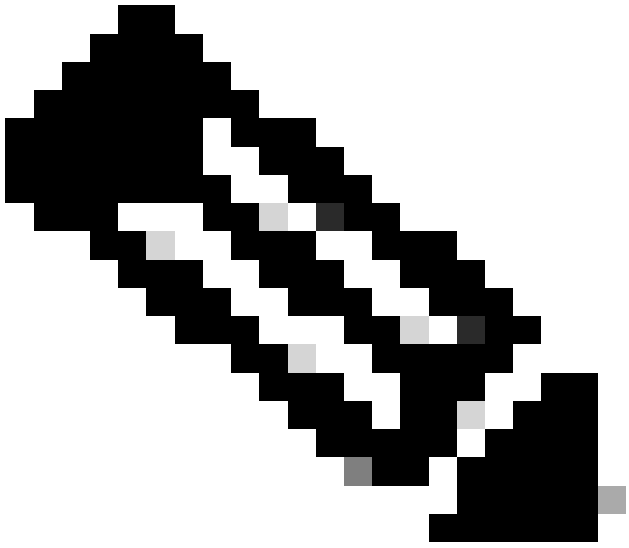
70단계(선택 사항) L4TM(Layer 4 Traffic Monitor)을 구성하려는 경우 Duplex 설정을 구성하거나, 기본값으로 두고 Next(다음)를 클릭할 수 있습니다.



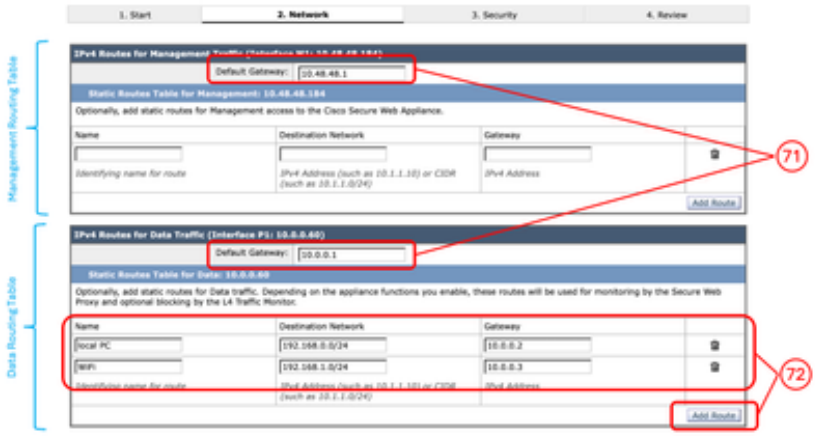
이미지 - 시스템 설정 마법사 - 레이어 4 트래픽 모니터 설정

71단계(선택 사항) Management(관리) 페이지의 IPv4 Routes(IPv4 경로)에서 Default Gateway(기본 게이트웨이)를 수정할 수 있습니다.

72단계(선택 사항) 고정 경로를 생성하기 위해 경로를 추가할 수 있습니다.

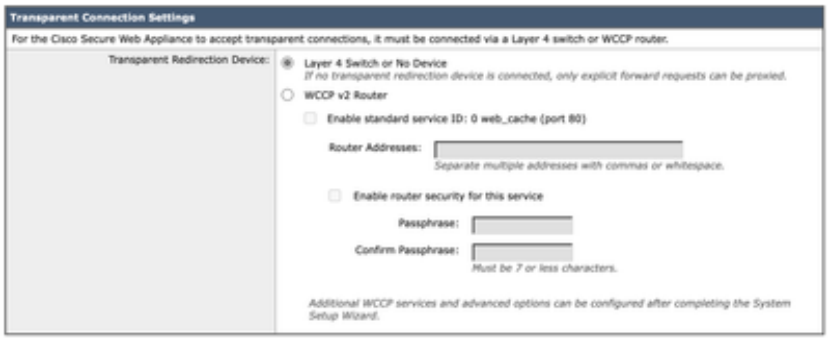


참고: 67단계에서 "Use M1 port for management only(관리에만 M1 포트 사용)"를 선택하면 관리 인터페이스 및 데이터 인터페이스(P1 및 P2)에 대해 두 개의 개별 라우팅 테이블이 있습니다.



이미지 - 시스템 설정 마법사 - 경로 추가

73단계(선택 사항) WCCP(Web Cache Communication Protocol)를 통해 투명 프록시 구축을 설정하려는 경우 WCCP 설정을 구성할 수 있습니다. 또는 기본 레이어 4 스위치 또는 장치 없음을 그대로 두고 Next(다음)를 클릭합니다.



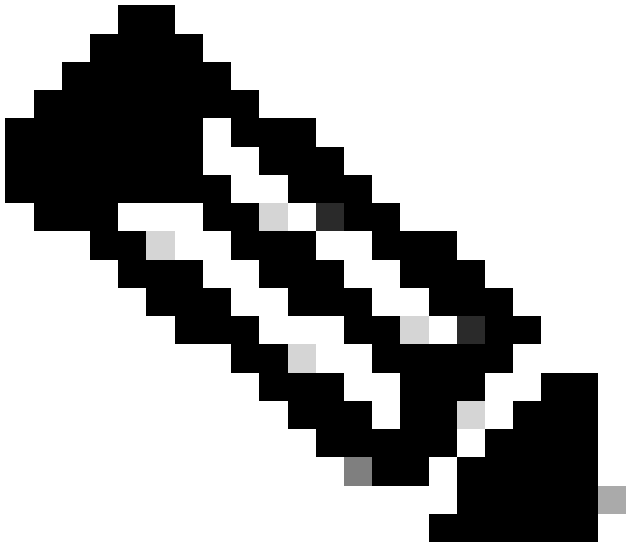
이미지 - 시스템 설정 마법사 - 프록시 구축 컨피그레이션

74단계. 관리자 계정에 대한 새 비밀번호를 설정합니다.

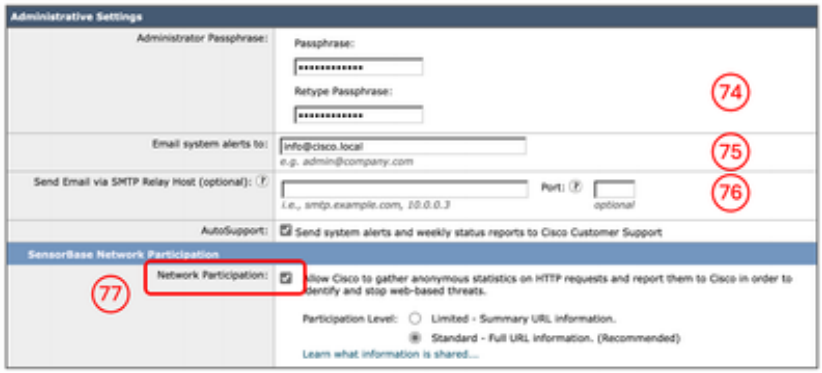
75단계. 시스템 알림을 수신할 이메일 주소를 입력합니다.

76단계(선택 사항) SMTP(Simple Mail Transfer Protocol) 릴레이 호스트 정보를 제공하거나 비워 둡니다 내부 릴레이 호스트가 정의되지 않은 경우 SMTP는 MX 레코드의 DNS 조회를 사용합니다.

77단계(선택 사항) Cisco SensorBase 네트워크에 참여를 비활성화하려면 Network Participation(네트워크 참여) 확인란의 선택을 취소하거나 기본값인 is를 그대로 두고 Next(다음)를 클릭합니다.

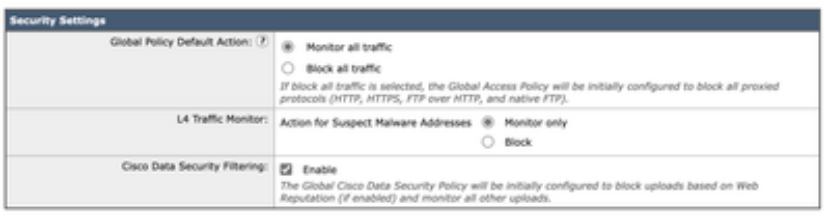


참고: Cisco SensorBase 네트워크에 참여한다는 것은 Cisco가 데이터를 수집하고 해당 정보를 SensorBase 위협 관리 데이터베이스와 공유한다는 의미입니다.



이미지 - 시스템 설정 마법사 - 관리 설정

78단계(선택 사항) Global Policy, L4TM 및 Cisco Data Security Filtering의 기본 작업을 변경할 수 있습니다. 또는 기본값으로 유지하고 Next(다음)를 클릭합니다.



이미지 - 시스템 설정 마법사 - 보안 설정

79단계. 컨피그레이션을 검토합니다. 변경해야 하는 경우

		이전 버튼을 클릭하여 이전 페이지로 돌아가거나, Install This Configuration(이 구성 설치)을 클릭합니다.

네트워크 설정

네트워크 인터페이스를 구성하려면 CLI 또는 GUI를 모두 사용할 수 있습니다.

	명령/경로	작업
CLI에서 네트워크 인터페이스 카드 구성	CLI > ifconfig	신규: 인터페이스가 ifconfig 출력에 나열되지 않았지만 가상 머신 또는 물리적 어플라이언스에 있는 경우 이 명령을 사용하여 목록에 인터페이스를 표시할 수 있습니다. Edit(수정): 이 작업은 IP 주소, 서브넷 마스크, 인터페이스 호스트 이름 또는 기타 관련 매개변수를 수정하는 것입니다. 세부사항: MAC 주소, 미디어 유형, 이중 모드 등의 인터페이스 세부사항을 표시합니다. Delete(삭제): ifconfig 목록에서 인터페이스를 제거하고, 이전에 할당한 경우 IP 주소를 제거합니다.
GUI에서 네트워크 인터페이스 카드 구성	GUI > Network > Interfaces	인터페이스 IP 주소 및 호스트 이름을 수정할 수 있습니다. 의 포트 번호를 활성화, 비활성화 또는 수정할 수 있습니다. FTP, SSH, HTTP 액세스 및 HTTPS 액세스와 같은 어플라이언스 관리 서비스

라우팅 테이블

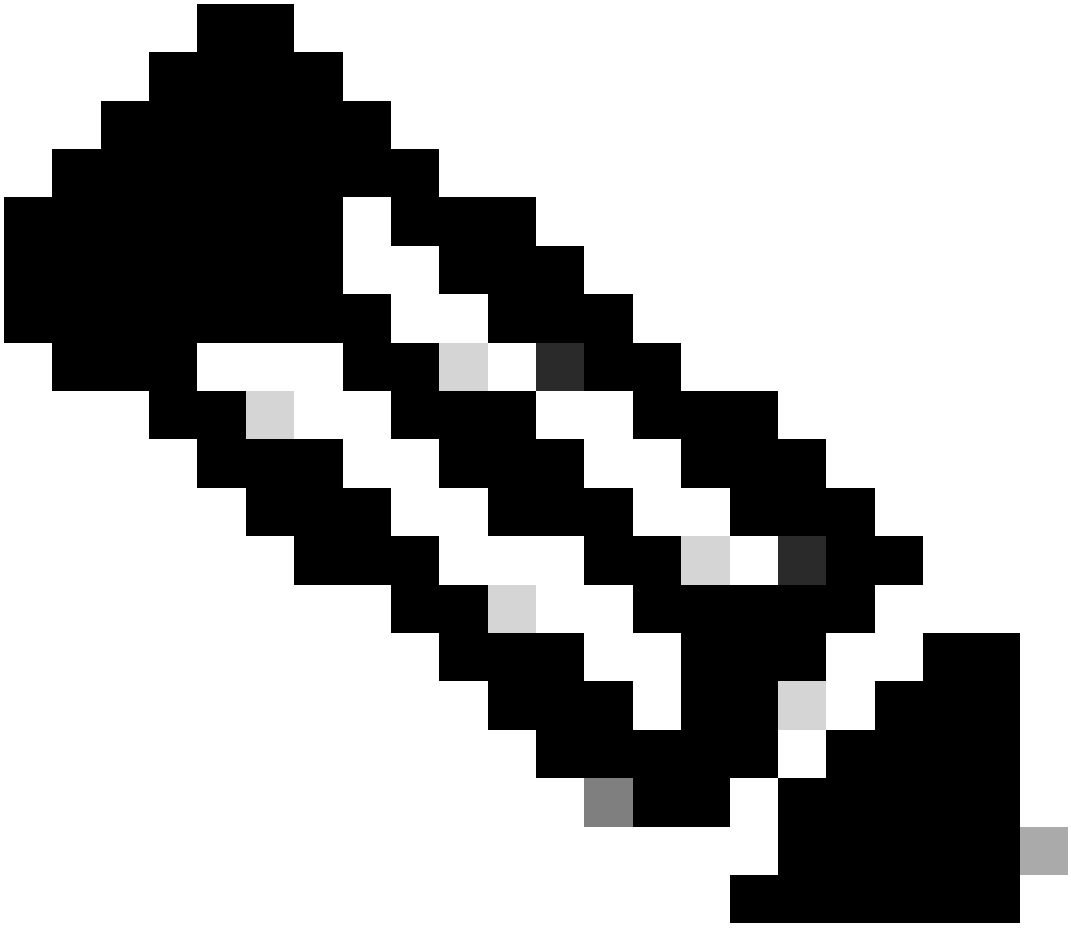
경로는 네트워크 트래픽을 어디로 전달할지 결정하는 데 필수적입니다. SWA는 다음 유형의 트래

픽을 처리합니다.

- 데이터 트래픽: 여기에는 인터넷을 탐색하는 최종 사용자의 웹 프록시에서 처리한 트래픽이 포함됩니다.
- 관리 트래픽: 웹 인터페이스를 통해 어플라이언스를 관리하여 생성된 트래픽은 물론 SWA 업그레이드, 구성 요소 업데이트, DNS, 인증 및 기타 관련 작업과 같은 관리 서비스에 대한 트래픽도 포함합니다.

기본적으로 두 트래픽 유형 모두 구성된 모든 네트워크 인터페이스에 대해 정의된 경로를 사용합니다. 그러나 관리 트래픽에서 전용 관리 라우팅 테이블을 사용하고 데이터 트래픽에서 별도의 데이터 라우팅 테이블을 사용하도록 라우팅을 분리하는 옵션이 있습니다.

관리 트래픽	데이터 트래픽
웹UI SSH SNMP 도메인 컨트롤러 사용 인증(구성 가능) Syslog FTP 푸시 DNS(구성 가능) 업데이트/업그레이드/기능 키(구성 가능)	HTTP 프록시 HTTPS 프록시 FTP 프록시 WCCP 협상 외부 DLP 서버와의 ICAP 요청 DNS(구성 가능) 업데이트/업그레이드/기능 키(구성 가능) 도메인 컨트롤러를 통한 인증(구성 가능)



참고: "Use M1 port for management only" 옵션을 선택하면 데이터 라우팅 테이블이라는 추가 라우팅 테이블이 SWA에 추가됩니다. 이 라우팅 테이블에는 구성 가능한 기본 게이트웨이가 하나만 있습니다. 추가 라우팅 경로는 수동으로 구성해야 합니다.

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서
- Cisco Secure Email and Web Virtual Appliance 설치 설명서
- Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco
- Secure Web Appliance 모범 사례 사용
- Secure Web Appliance용 방화벽 구성
- Secure Web Appliance에서 암호 해독 인증서 구성
- SWA에서 SNMP 구성 및 문제 해결

- Microsoft Server를 사용하여 Secure Web Appliance에서 SCP 푸시 로그 구성
- SWA에서 특정 YouTube 채널/비디오 활성화 및 나머지 YouTube 차단
- Secure Web Appliance의 HTTPS 액세스 로그 형식 이해
- Secure Web Appliance 로그 액세스
- Secure Web Appliance에서 인증 우회
- Secure Web Appliance에서 트래픽 차단
- Secure Web Appliance에서 Microsoft 업데이트 트래픽 우회

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.