ASDM을 통한 ASA 구축

이 장의 설명이 유용합니까?

사용 가능한 모든 운영 체제 및 관리자를 보려면 귀하에게 적합한 애플리케이션 및 관리자는 무엇입니까? 항목을 참조하십시오. 이 장은 ASDM을 사용하는 ASA에 적용됩니다.

방화벽 정보

하드웨어는 ASA 소프트웨어 또는 threat defense 소프트웨어를 실행할 수 있습니다. ASA와 threat defense 간 전환하려면 디바이스에 이미지를 재설치해야 합니다. 현재 설치된 것과 다른 소프트웨어 버전이 필요한 경우에도 이미지를 재설치해야 합니다. Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드의 내용을 참조하십시오.

방화벽은 Secure Firewall eXtensible Operating System(FXOS)라는 기본 운영 체제를 실행합니다. 방화벽은 FXOS Secure Firewall 섀시 관리자를 지원하지 않습니다. 문제 해결을 위해 제한된 CLI만 지원됩니다. 자세한 내용은 Cisco Firepower 1000/2100 및 Firepower Threat Defense 기능이 있는 Threat Defense 3100/4200용 Cisco FXOS 문제 해결 가이드을 참조하십시오.

Privacy Collection Statement(개인정보 수집 선언**)**—방화벽은 개인 식별 정보를 요구하거나 적극적으로 수집하지 않습니다. 그러나 구성에서 개인 식별이 가능한 정보(예: 사용자 이름)를 사용할 수 있습니다. 이 경우 관리자는 해당 설정으로 작업하거나 SNMP를 사용할 때 이 정보를 확인할 수도 있습니다.

ASA 정보

ASA는 고급 스테이트풀 방화벽 및 VPN 집중기 기능을 하나의 디바이스에서 제공하며

ASA 5500-X 설정 마이그레이션

ASA 5500-X의 설정을 복사하여 Secure Firewall 4200에 붙여 넣을수 있습니다. 그러나 구성을 수정할 필요가 있습니다. 또한 플랫폼 간 몇 가지 동작 차이가 있습니다.

1. 설정을 복사하려면 ASA 5500-X에 **more system:running-config** 명령을 입력합니다.
2. 필요에 따라 구성을 수정합니다(아래 참조).
3. Secure Firewall 4200의 콘솔 포트에 연결하고 전역 구성 모드를 입력합니다.

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. **clear configure all** 명령을 사용하여 현재 설정을 지웁니다.
5. ASA CLI에 수정된 설정을 붙여넣습니다.

이 가이드에서는 공장 기본 설정을 가정하므로 기존 설정에 붙여넣으면 이 가이드의 절차 중 일부가 ASA에 적용되지 않습니다.

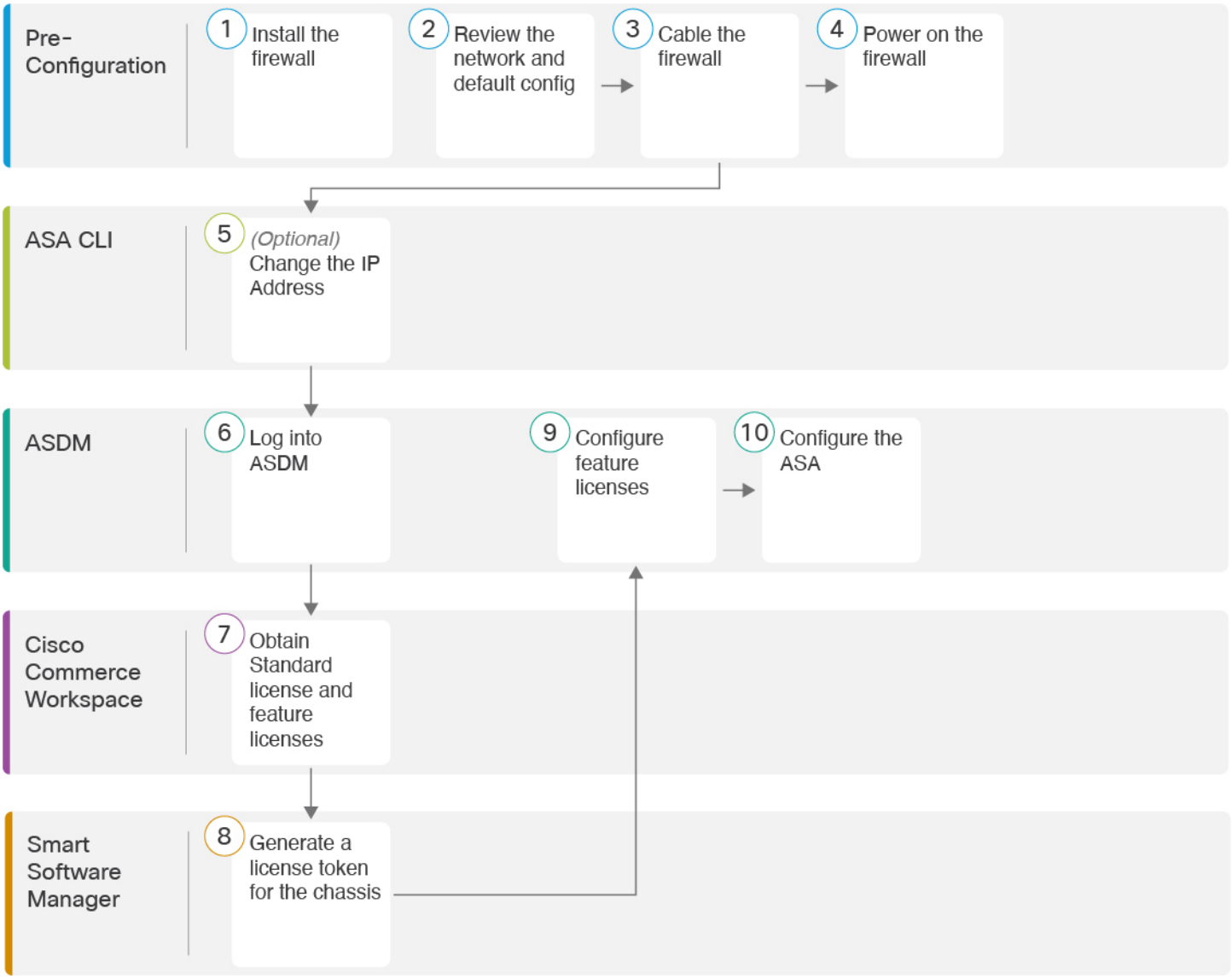
ASA 5500-X 설정	Secure Firewall 4200 구성
PAK 라이선스	스마트 라이선스 설정을 복사하여 붙여 넣을 때에는 PAK 라이선스가 적용되지 않습니다. 기본적으로 설치된 라이선스가 없습니다. 스마트 라이선싱을 사용하려면 스마트 라이선싱 서버에 연결하여 라이선스를 얻어야 합니다. 스마트 라이선싱은 ASDM이나 SSH 액세스에도 영향을 미칩니다(아래 참조).

ASA 5500-X 설정	**Secure Firewall 4200** 구성
최초 ASDM 액세스	약한 암호화만 설정한 경우에도 VPN 또는 다른 강력한 암호화 기능 설정을 제거합니다. ASDM에 연결할 수 없거나 스마트 라이선싱 서버에 등록할 수 없는 경우에도 해당합니다. 강력한 암호화(3DES) 라이선스를 얻은 후 이러한 기능을 다시 활성화할 수 있습니다. 이 문제가 발생하는 이유는 ASA가 관리 액세스 전용으로 3DES 기능을 기본적으로 포함하기 때문입니다. 강력한 암호화 기능을 활성화하면 ASDM 및 HTTPS 트래픽(스마트 라이선싱 서버와 유사)이 차단됩니다. 관리 전용 인터페이스(예: 관리 1/1)에 연결되어 있는 경우에는 이 규칙의 예외가 적용됩니다. SSH는 영향을 받지 않습니다.
인터페이스 ID	새 하드웨어 ID와 일치하도록 인터페이스 ID를 변경해야 합니다. 예를 들어 ASA 5525-X는 관리 0/0을, GigabitEthernet은 0/0~0/5를 포함합니다. Firepower 1120에는 관리 1/1 및 Ethernet 1/1~1/8이 포함됩니다.
boot system 명령 ASA 5500-X에서는 최대 4개의 **boot system** 명령을 사용하여 사용할 부팅 이미지를 지정할 수 있습니다.	Secure Firewall 4200에서는 단일 **boot system** 명령만 허용하므로 복사해서 붙여 넣기 전에 명령을 하나만 남기고 전부 제거해야 합니다. 시작 시 부팅 이미지를 확인하기 위해 이를 읽어들이지 않으므로 실제로는 설정에 어떤 **boot system** 명령도 필요하지 않습니다. 마지막으로 로드된 부팅 이미지는 재로드 시 항상 실행됩니다. **boot system** 명령은 입력 시 작업을 수행합니다. 시스템은 이미지의 유효성을 검사하고 압축을 푼 뒤 부팅 위치(FXOS가 관리하는 disk0의 내부 위치)에 이를 복사합니다. 새 이미지는 ASA를 다시 로드할 때 로드됩니다.

엔드 투 엔드 작업

섀시에 ASA를 구축하고 구성하려면 다음 작업을 참조하십시오.

그림 *1:* 엔드 투 엔드 작업



1	사전 컨피그레이션	방화벽을 설치합니다. 하드웨어 설치 가이드를 참조하십시오.
2	사전 컨피그레이션	네트워크 구축 및 기본 구성 검토, 5 페이지에 전달하는 고성능 고속 어플라이언스입니다.
3	사전 컨피그레이션	방화벽 케이블 연결, 7 페이지에 전달하는 고성능 고속 어플라이언스입니다.
4	사전 컨피그레이션	Firewall 켜기, 8 페이지에 전달하는 고성능 고속 어플라이언스입니다.
5	ASA CLI	(선택 사항) IP 주소 변경, 9 페이지에 전달하는 고성능 고속 어플라이언스입니다.

6	ASDM	ASDM에 로그인, 10 페이지에 전달하는 고성능 고속 어플라이언스입니다.
7	Cisco Commerce Workspace	Standard 라이선스 및 선택적 기능 라이선스를 얻습니다(라이선싱 구성, 11 페이지).
8	Smart Software Manager	섀시에 대한 라이선스 토큰을 생성합니다(라이선싱 구성, 11 페이지).
9	ASDM	기능 라이선스를 구성합니다(라이선싱 구성, 11 페이지).
10	ASDM	ASA 구성, 17 페이지.

네트워크 구축 및 기본 구성 검토

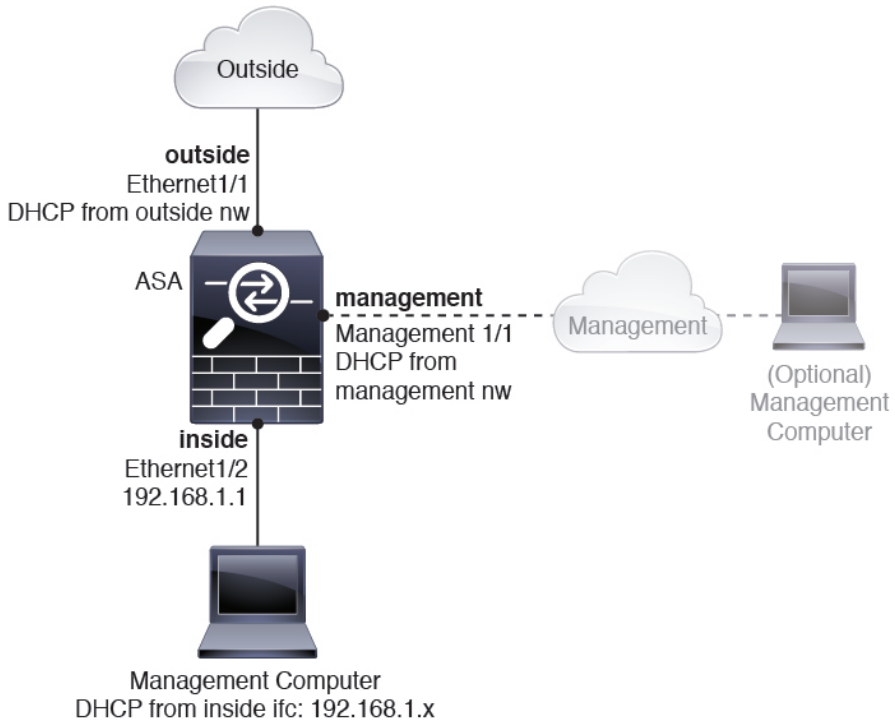
다음 그림에는 에서의 기본 설정을 사용한 ASA의 기본 네트워크 구축이 나와 있습니다.

외부 인터페이스를 케이블 모뎀 또는 DSL 모뎀에 직접 연결하는 경우에는 ASA가 내부 네트워크에 대해 모든 라우팅 및 NAT를 수행하도록 모뎀을 브리지 모드로 설정하는 것이 좋습니다. ISP에 연결하기 위해 외부 인터페이스에 대해 PPPoE를 구성해야 하는 경우 ASDM 시작 마법사의 일부로 수행할 수 있습니다.

참고 ASDM 액세스에 기본 관리 IP 주소를 사용할 수 없는 경우 ASA CLI에서 관리 IP 주소를 설정할 수 있습니다. (선택 사항) IP 주소 변경, 9 페이지의 내용을 참조하십시오.

내부 IP 주소를 변경해야 하는 경우 ASDM 시작 마법사를 사용하여 변경할 수 있습니다. 예를 들어 다음과 같은 상황에서는 내부 IP 주소를 변경해야 할 수 있습니다.

- 외부 인터페이스가 공통 기본 네트워크인 192.168.1.0 네트워크에서 IP 주소를 얻으려고 시도하면 DHCP 리스가 실패하고 외부 인터페이스가 IP 주소를 가져오지 않습니다. 이 문제는 ASA가 동일한 네트워크에 두 개의 인터페이스를 가질 수 없기 때문에 발생합니다. 이 경우 새 네트워크에 있도록 내부 IP 주소를 변경해야 합니다.
- 기존 내부 네트워크에 ASA를 추가하는 경우 내부 IP 주소를 기존 네트워크에 있도록 변경해야 합니다.



Secure Firewall 4200 기본 구성

Secure Firewall 4200의 기본 공장 구성은 다음을 구성합니다.

- 내부→외부 트래픽 플로우—Ethernet 1/1(외부), Ethernet 1/2(내부)
- DHCP로부터의 외부 **IP** 주소, 내부 **IP** 주소—192.168.1.1
- 관리—관리 1/1 (관리), DHCP에서 제공된 IP 주소
- 내부 인터페이스의 **DHCP** 서버
- 외부 DHCP의 기본 경로, 관리 DHCP
- **ASDM** 액세스—관리 및 내부 호스트가 허용됩니다. 내부 호스트는 192.168.1.0/24 네트워크로 제한됩니다.
- **NAT**—내부에서 외부로 가는 모든 트래픽을 위한 인터페이스 PAT.
- **DNS** 서버—OpenDNS 서버는 사전에 구성되어 있습니다.

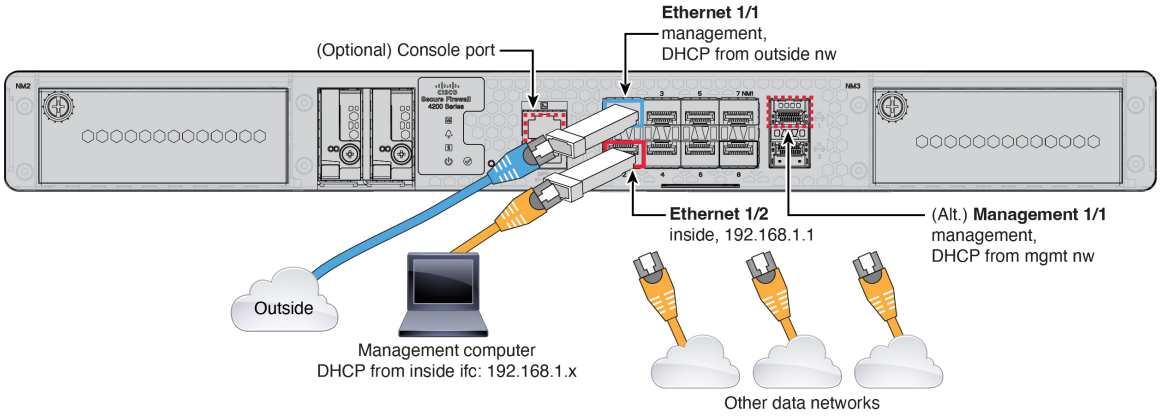
컨피그레이션은 다음 명령으로 구성됩니다.

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
```

```
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

방화벽 케이블 연결

그림 ***2: Secure Firewall 4200*** 케이블 연결



관리 1/1 또는 이더넷 1/2에서 Secure Firewall 4200을 관리합니다. 기본 구성에서는 Ethernet1/1을 외부로도 구성합니다.

시작하기 전에

- 데이터 인터페이스 및 옵션 관리 포트에 SFP 설치 - 기본 제공 포트는 SFP 모듈이 필요한 1/10/25-Gb SFP 포트입니다.
- (선택 사항) 콘솔 케이블 얻기 - 방화벽은 기본적으로 콘솔 케이블과 함께 제공되지 않으므로 예를 들어 서드파티 USB-RJ-45 직렬 케이블을 구매해야 합니다.

프로시저

단계 **1** 섀시를 설치합니다. 하드웨어 설치 가이드를 참조하십시오.

단계 **2** 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.

- **Ethernet 1/2**—기본 IP 주소(192.168.1.1)가 있는 Ethernet 1/2에서는 DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다(Secure Firewall 4200 기본 구성, 6 페이지 참조). 192.168.1.0/24의 클라이언트만 ASA에 액세스할 수 있습니다.

  Ethernet 1/2 IP 주소를 기본값에서 변경해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) IP 주소 변경, 9 페이지의 내용을 참조하십시오.
- 관리 **1/1**—관리 1/1은 관리 네트워크의 DHCP 서버에서 IP 주소를 가져옵니다. 이 인터페이스를 사용하는 경우 관리 컴퓨터에서 해당 IP 주소에 연결할 수 있도록 ASA에 할당된 IP 주소를 확인해야 합니다.

  나중에 다른 관리 인터페이스가 필요한 경우 관리 1/2를 설정할 수 있습니다.

나중에 다른 인터페이스에서 ASA 관리 액세스를 구성할 수 있습니다. ASA 일반 운영 구성 가이드를 참조하십시오.

단계 **3** Ethernet1/1 인터페이스에 외부 네트워크를 연결합니다.

스마트 소프트웨어 라이선싱의 경우 ASA에는 인터넷 액세스가 필요합니다.

단계 **4** 나머지 인터페이스에 다른 네트워크를 연결합니다.

Firewall 켜기

시스템 전원은 디바이스 뒷면에 있는 로커 전원 스위치로 제어됩니다. 전원 스위치는 정상적인 종료를 지원하는 소프트 알림 스위치로 구현되어 시스템 소프트웨어 및 데이터 손상의 위험을 줄여줍니다.

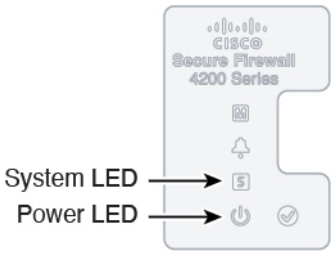
프로시저

단계 **1** 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.

단계 **2** 전원 코드 옆 섀시 후면에 있는 표준 로커 유형 전원 켜기/끄기 스위치를 사용하여 전원을 켭니다.

단계 **3** 방화벽 뒷면의 전원 LED를 확인합니다. 전원이 켜져 있으면 녹색으로 표시됩니다.

그림 *3:* 시스템 및 전원 ***LED***



단계 **4** 방화벽 뒷면의 시스템 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

참고 스위치가 ON(켜짐)에서 OFF(꺼짐)로 토글된 경우 시스템에서 최종적으로 전원이 꺼지는 데 몇 초 정도가 걸릴 수 있습니다. 이 시간 동안 섀시 전면에 있는 전원 LED가 녹색으로 깜박입니다. 전원 LED가 완전히 꺼질 때까지 전원을 제거하지 마십시오.

(선택 사항) IP 주소 변경

ASDM 액세스에 기본 IP 주소를 사용할 수 없는 경우 ASA CLI에서 내부 인터페이스의 IP 주소를 설정할 수 있습니다.

참고 이 절차에서는 기본 구성을 복원하고 선택한 IP 주소도 설정하므로 보존하려는 ASA 구성을 변경한 경우 이 절차를 사용하지 마십시오.

프로시저

단계 **1** ASA 콘솔 포트에 연결한 다음 전역 구성 모드를 설정합니다. 자세한 내용은 의 ASA 및 FXOS CLI 액세스, 19 페이지을/를 참조하십시오.

단계 **2** 선택한 IP 주소로 기본 구성을 복원합니다.

configure factory-default [*ip_address* [*mask*]]

예제:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
```

```
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

단계 **3** 플래시 메모리에 기본 컨피그레이션을 저장합니다.

write memory

ASDM에 로그인

ASDM을 시작하여 ASA를 구성할 수 있습니다.

ASA는 기본적으로 관리 액세스용으로만 3DES 기능을 포함하므로 Smart Software Manager에 연결하고 ASDM을 즉시 사용할 수도 있습니다. 이후 ASA에서 SSH 액세스를 구성하는 경우, SSH와 SCP도 사용할 수 있습니다. 강력한 암호화(예: VPN)가 필요한 기타 기능을 사용하려면 먼저 Smart Software Manager에 등록이 필요한 강력한 암호화가 활성화되어 있어야 합니다.

참고 약한 암호화만 구성하는 경우에도 등록 전에 강력한 암호화를 사용할 수 있는 기능을 구성하려고 시도하는 경우 HTTPS 연결이 해당 인터페이스에서 제거되므로 다시 연결할 수 없습니다. 관리 전용 인터페이스(예: 관리 1/1)에 연결되어 있는 경우에는 이 규칙의 예외가 적용됩니다. SSH는 영향을 받지 않습니다. HTTPS 연결이 끊기면 콘솔 포트에 연결하여 ASA를 재구성하거나, 관리 전용 인터페이스에 연결하거나, 강력한 암호화 기능으로 구성되지 않은 인터페이스에 연결할 수 있습니다.

시작하기 전에

- ASDM을 실행하기 위한 요구 사항은 Cisco.com의 ASDM 릴리스 노트를 참조하십시오.

프로시저

단계 **1** 브라우저에 다음 URL을 입력합니다.

- **https://192.168.1.1**—내부(Ethernet 1/2) 인터페이스 IP 주소입니다.
- **https://***management_ip*—DHCP에서 할당된 관리 인터페이스 IP 주소입니다.

참고 **http://**가 아닌 **https://**를 지정하거나 IP 주소(기본값은 HTTP)만 지정해야 합니다. ASA에서는 HTTP 요청을 HTTPS로 자동으로 전달하지 않습니다.

Cisco ASDM 웹 페이지가 나타납니다. ASA에 인증서가 설치되어 있지 않아 브라우저 보안 경고가 표시될 수 있습니다. 이 경고를 무시하고 웹 페이지를 방문할 수 있습니다.

단계 **2** **Install ASDM Launcher(ASDM Launcher** 설치**)**를 클릭합니다.

단계 **3** ASDM을 구동하기 위한 화면의 지침을 수행합니다.

Cisco ASDM-IDM Launcher가 나타납니다.

단계 **4** 사용자 이름 및 비밀번호 필드를 비워두십시오 **OK(**확인**)**을 클릭합니다.

기본 ASDM 창이 나타납니다.

라이선싱 구성

ASA은 스마트 라이선싱을 사용합니다. 인터넷 액세스가 필요한 일반 스마트 라이선싱을 사용하거나 오프라인 관리를 위해 영구 라이선스 예약 또는 Smart Software Manager ON-Prem(구 Satellite 서버)을 구성할 수 있습니다. 이러한 오프라인 라이선싱 방법에 대한 자세한 내용은 Cisco ASA Series 기능 라이선스를 참조하십시오. 이 가이드는 일반 스마트 라이선싱에 적용됩니다.

시스코 라이선싱에 대한 자세한 내용은 cisco.com/go/licensingguide를 참조하세요.

섀시를 등록할 때 Smart Software Manager는 방화벽과 Smart Software Manager 간의 통신을 위해 ID 인증서를 발급합니다. 또한 방화벽를 적절한 가상 어카운트에 지정합니다. Smart Software Manager에 등록할 때까지 구성을 변경할 수 없으며 그 외에는 작업은 달리 영향을 받지 않습니다. 라이선스가 있는 기능은 다음과 같습니다.

- Essentials
- 보안 상황
- Carrier—배율, GTP/GPRS, M3UA, SCTP
- 강력한 암호화(3DES/AES) - 스마트 어카운트가 강력한 암호화에 대해 인증되지 않았지만 Cisco에서 강력한 암호화를 사용할 수 있다고 결정한 경우, 수동으로 어카운트에 강력한 암호화 라이선스를 추가할 수 있습니다.
- Cisco Secure Client—Secure Client Advantage, Secure Client Premier 또는 Secure Client VPN 전용

ASA는 기본적으로 관리 액세스용으로만 3DES 기능을 포함하므로 Smart Software Manager에 연결하고 ASDM을 즉시 사용할 수도 있습니다. 이후 ASA에서 SSH 액세스를 구성하는 경우, SSH와 SCP도 사용할 수 있습니다. 강력한 암호화(예: VPN)가 필요한 기타 기능을 사용하려면 먼저 Smart Software Manager에 등록이 필요한 강력한 암호화가 활성화되어 있어야 합니다.

참고 약한 암호화만 구성하는 경우에도 등록 전에 강력한 암호화를 사용할 수 있는 기능을 구성하려고 시도하는 경우 HTTPS 연결이 해당 인터페이스에서 제거되므로 다시 연결할 수 없습니다. 관리 전용 인터페이스(예: 관리 1/1)에 연결되어 있는 경우에는 이 규칙의 예외가 적용됩니다. SSH는 영향을 받지 않습니다. HTTPS 연결이 끊기면 콘솔 포트에 연결하여 ASA를 재구성하거나, 관리 전용 인터페이스에 연결하거나, 강력한 암호화 기능으로 구성되지 않은 인터페이스에 연결할 수 있습니다.

Smart Software Manager에서 ASA에 대한 등록 토큰을 요청할 때 **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** 체크 박스를 선택하여 강력한 암호화 라이선스 전체를 적용하십시오(사용하기 위해서는 계정이 유효해야 함). 사용자가 새시에 등록 토큰을 적용하면 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화되므로 추가 작업이 필요하지 않습니다. 스마트 어카운트가 강력한 암호화에 대해 인증되지 않았지만 Cisco에서 강력한 암호화를 사용할 수 있다고 결정한 경우, 수동으로 어카운트에 강력한 암호화 라이선스를 추가할 수 있습니다.

시작하기 전에

- Cisco Smart Software Manager에서 마스터 계정을 만듭니다.

  아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

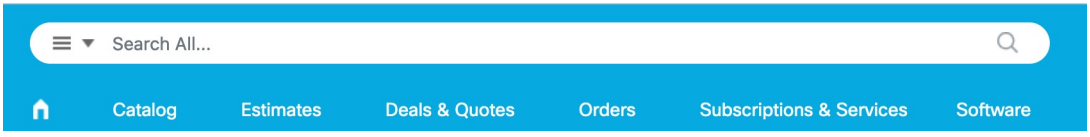
- Smart Software Manager 계정에서 일부 기능(내보내기-컴플라이언스 플래그를 사용하여 활성화됨)을 사용하려면 강력한 암호화(3DES/AES) 라이선스 자격을 얻어야 합니다.

프로시저

단계 **1** 스마트 라이선싱 계정에서 필요한 라이선스(최소 Essentials 라이선스 포함)가 사용 가능한 상태인지 확인합니다.

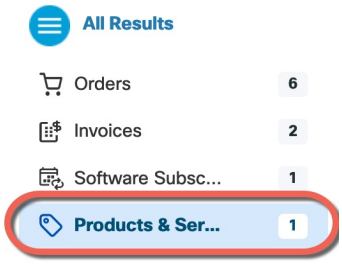
Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace에서 **Search All(**모두 검색**)** 필드를 사용합니다.

그림 *4:* 라이선스 검색



결과에서 **Products & Services(**제품 및 서비스**)**를 선택합니다.

그림 *5:* 결과



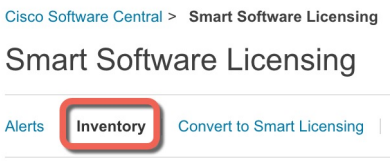
다음 라이선스 PID를 검색합니다.

참고 PID를 찾을 수 없는 경우 주문에 수동으로 PID를 추가할 수 있습니다.

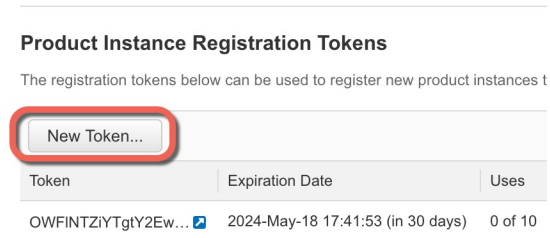
- Essentials 라이선스—L-FPR4215-BSE=. Essentials 라이선스는 필수 라이선스입니다.
- Essentials 라이선스—L-FPR4225-BSE=. Essentials 라이선스는 필수 라이선스입니다.
- Essentials 라이선스—L-FPR4245-BSE=. Essentials 라이선스는 필수 라이선스입니다.
- 5개의 상황 라이선스—L-FPR4200-ASASC-5=. 상황 라이선스는 부가 라이선스입니다. 요구 사항에 맞게 여러 라이선스를 구매하십시오.
- 10개의 상황 라이선스—L-FPR4200-ASASC-10=. 상황 라이선스는 부가 라이선스입니다. 요구 사항에 맞게 여러 라이선스를 구매하십시오.
- 캐리어(배율, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=입니다.
- 강력한 암호화(3DES/AES) 라이선스—L-FPR4200-ENC-K9=입니다. 해당 스마트 어카운트에 강력한 암호화에 대한 권한이 없는 경우에만 필요합니다.
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참조하십시오. ASA에서 직접 이 라이선스를 활성화하지 마십시오.

단계 **2** Cisco Smart Software Manager에서 이 디바이스를 추가할 가상 어카운트에 대한 등록 토큰을 요청 및 복사합니다.

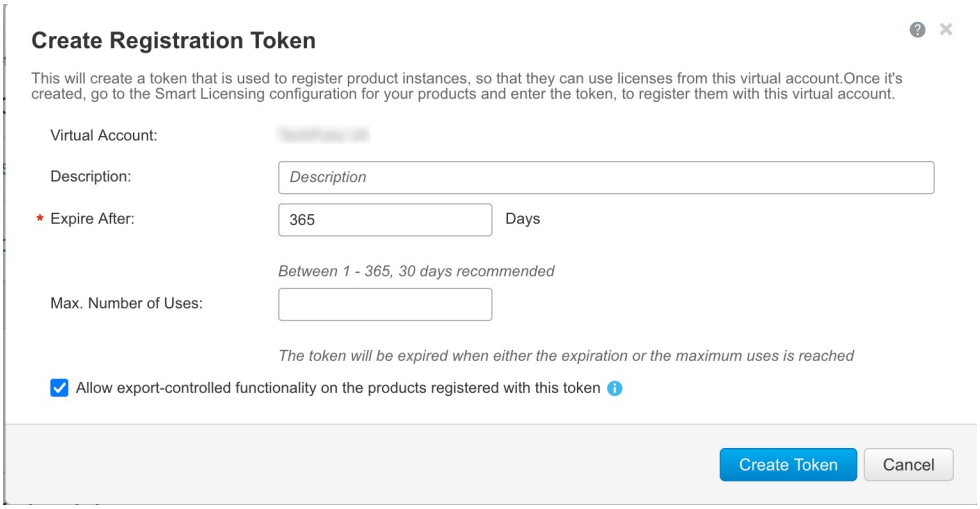
a) **Inventory(**인벤토리**)**를 클릭합니다.



b) **General(**일반**)** 탭에서 **New Token(**새 토큰**)**을 클릭합니다.



c) **Create Registration Token(**등록 토큰 생성**)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(**토큰 생성**)**을 클릭합니다.



- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.
- 최대 사용 개수
- **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** — export-compliance 플래그를 활성화합니다.

토큰이 인벤토리에 추가됩니다.

d) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(**토큰**)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 ASA를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

그림 *6:* 토큰 보기

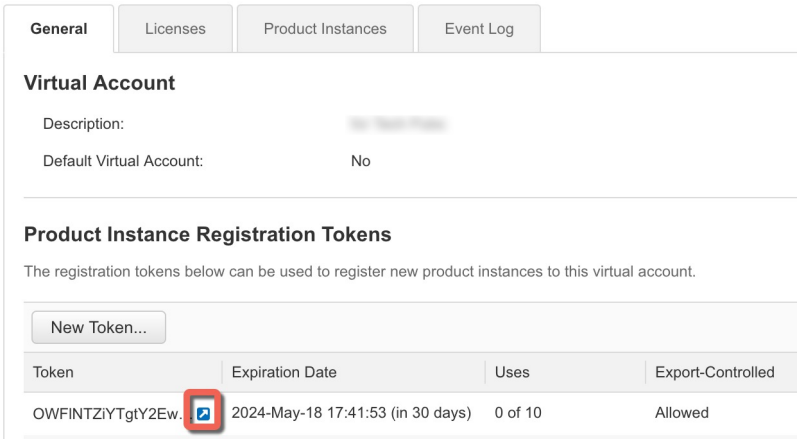
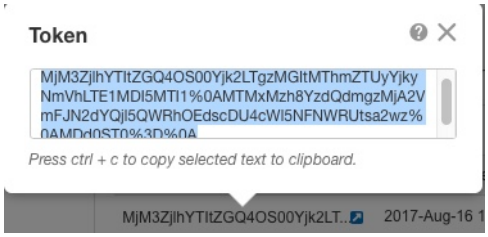
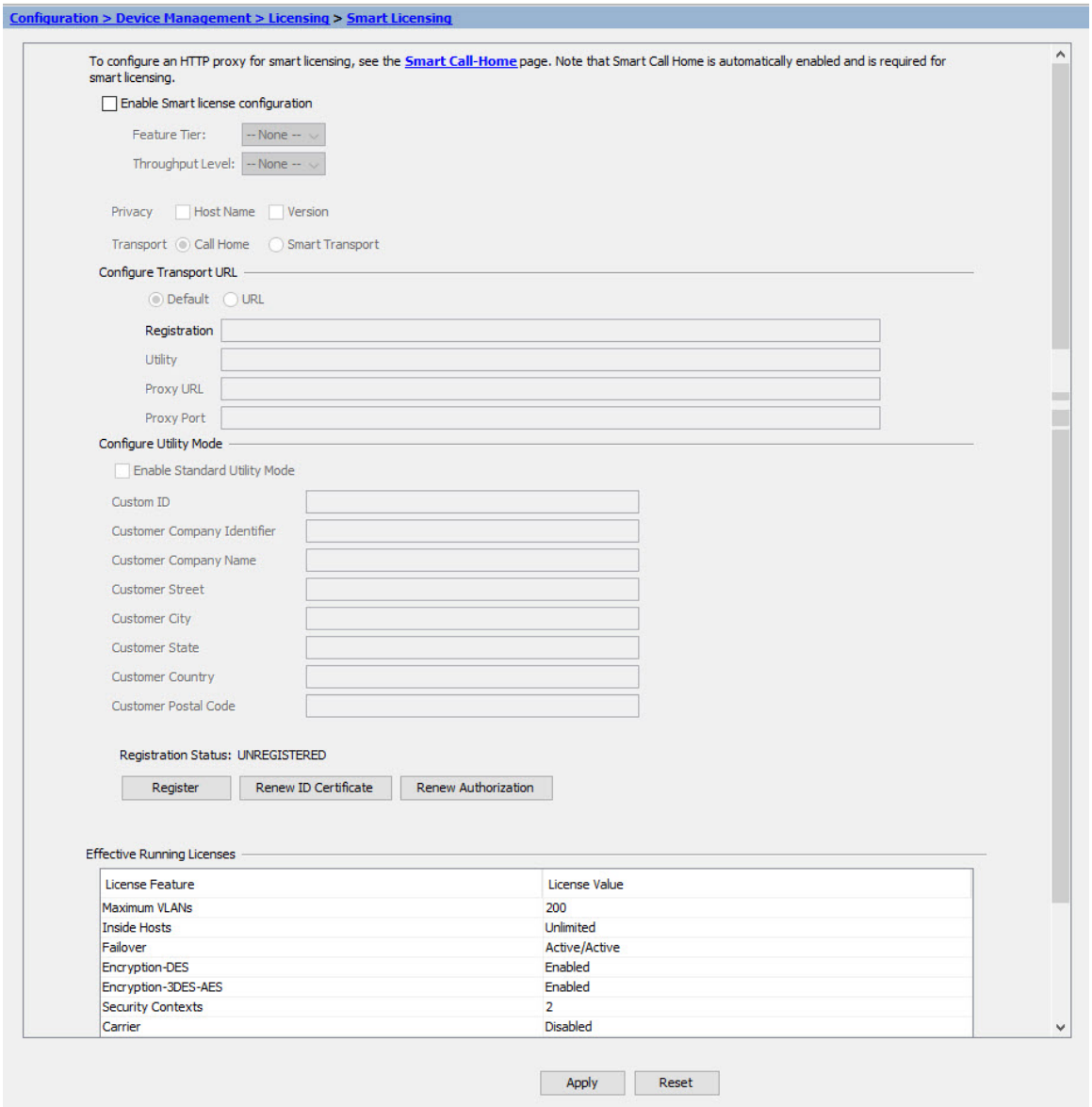


그림 *7:* 토큰 복사

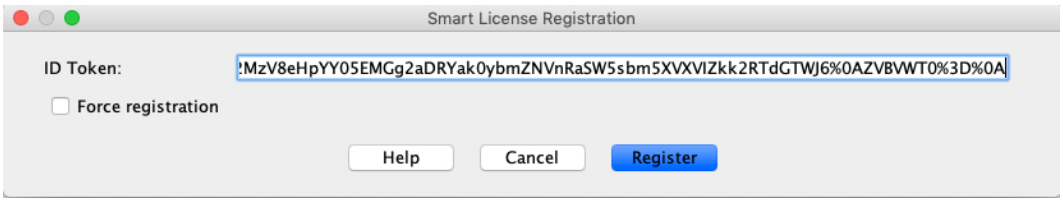


단계 **3** ASDM에서 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **Licensing(**라이선싱**)** > **Smart Licensing(**스마트 라이선싱**)**을 선택합니다.

단계 **4** **Register(**등록**)**를 클릭합니다.



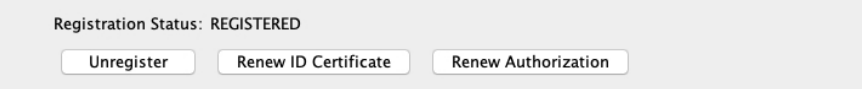
단계 **5** **ID Token(ID** 토큰**)** 필드에 등록 토큰을 입력합니다.



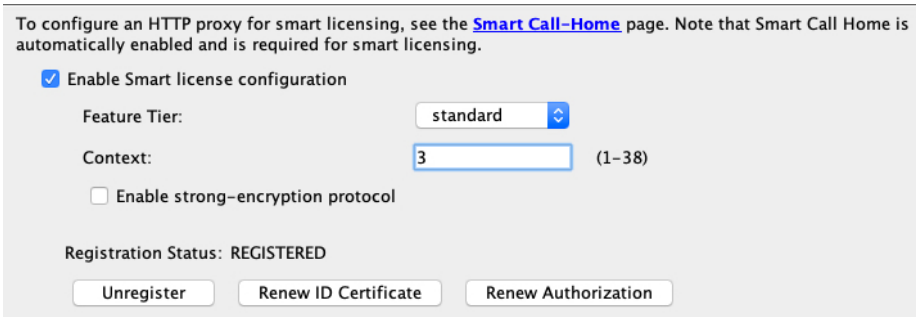
(선택 사항) 이미 등록되었지만 Smart Software Manager와 동기화되지 않았을 수 있는 ASA를 등록하려면 **Force Registration(**강제 등록**)** 체크 박스를 클릭합니다. 예를 들어 ASA가 Smart Software Manager에서 실수로 제거된 경우 **Force registration(**등록 강제 적용**)**을 사용하십시오.

단계 **6** **Register(**등록**)**를 클릭합니다.

ASA를 사전 구성된 외부 인터페이스를 사용하는 Smart Software Manager에 등록하고 구성된 라이선스 자격에 대한 권한 부여를 요청합니다. 어카운트에서 허용하는 경우 Smart Software Manager는 강력한 암호화(3DES/AES) 라이선스도 적용합니다. 라이선스 상태가 업데이트되면 ASDM에서 페이지를 새로 고칩니다. 또한 **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Smart License**를 선택하여 라이선스 상태, 특히 등록이 실패하였는지 여부를 확인할 수 있습니다.



단계 **7** 다음 매개변수를 설정합니다.



a) **Enable Smart license configuration(**스마트 라이선스 컨피그레이션 활성화**)**을 선택합니다.

b) **Feature Tier(**기능 계층**)** 드롭다운 목록에서 **Essentials**를 선택합니다.

Essentials 계층만 사용 가능합니다.

c) (선택 사항) 상황 라이선스의 경우 상황 수를 입력합니다.

- Secure Firewall 4200 - 100개의 상황

예를 들어, Secure Firewall 4215에서 최대 100개의 상황을 사용하려면 상황 수에 98을 입력합니다. 이 값은 기본값 2에 추가됩니다.

단계 **8** **Apply(**적용**)**를 클릭합니다.

단계 **9** 툴바에서 **Save(**저장**)** 아이콘을 클릭합니다.

단계 **10** ASDM을 종료하고 다시 실행합니다.

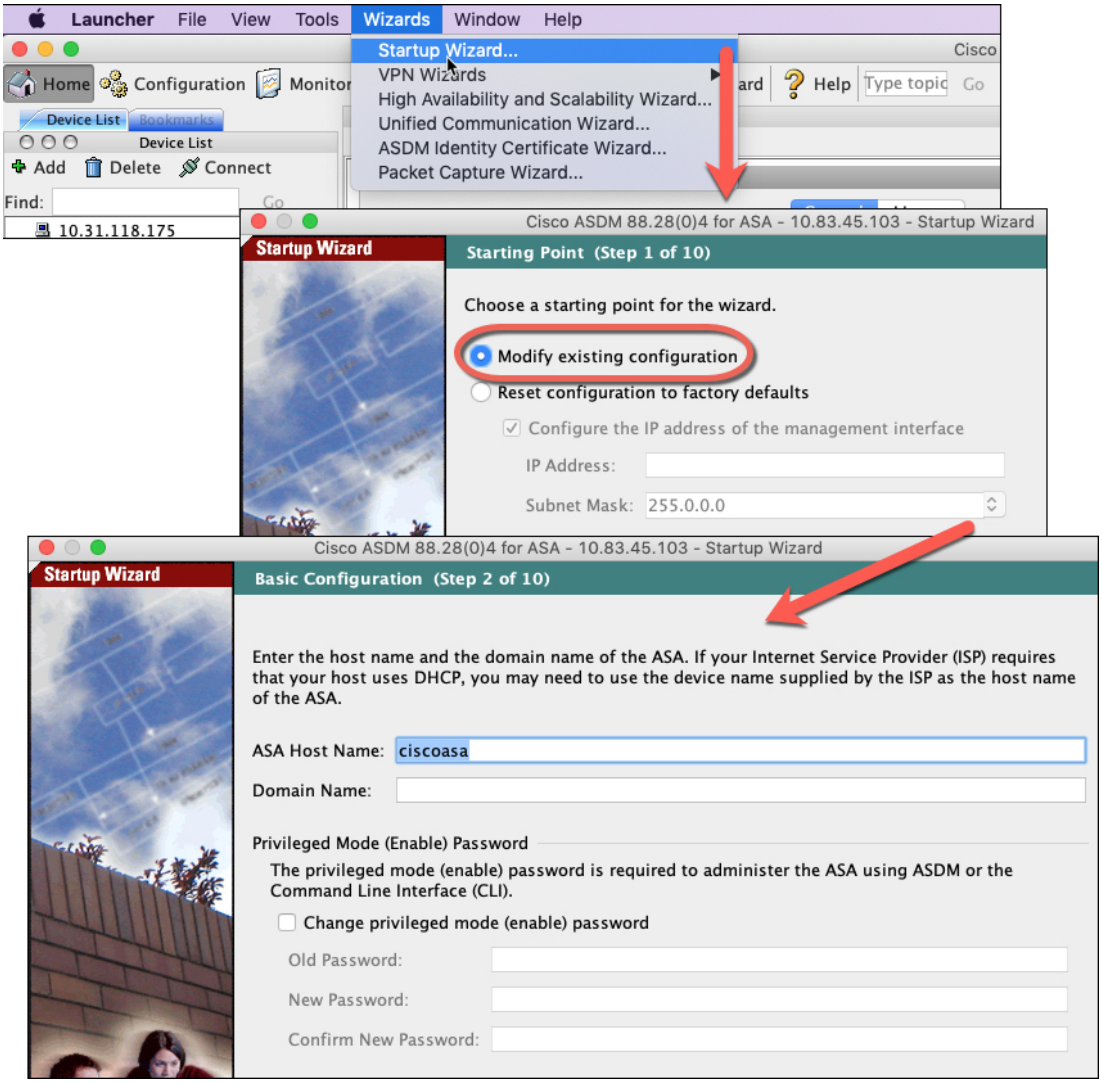
라이선스를 변경하면 업데이트된 화면을 표시하기 위해 ASDM을 다시 실행해야 합니다.

ASA 구성

ASDM을 사용하면 마법사를 통해 기본 및 고급 기능을 구성할 수 있습니다. 또한, 수동으로 마법사에 포함되지 않은 기능을 구성할 수 있습니다.

프로시저

단계 **1** **Wizards(**마법사**) > Startup Wizard(**시작 마법사**)**를 클릭하고 **Modify existing configuration(**기존 컨피그레이션 수정**)** 라디오 버튼을 클릭합니다.



단계 **2** **Startup Wizard(**시작 마법사**)**에서는 다음 항목을 구성하는 방법을 안내합니다.

- 활성화 비밀번호
- 인터페이스(내부 및 외부 인터페이스 IP 주소 및 인터페이스 활성화 포함)
- 정적 경로
- DHCP 서버
- 기타...

단계 3 (선택 사항) **Wizards(**마법사**)** 메뉴에서 다른 마법사를 실행합니다.

단계 4 ASA를 계속 구성하려면 Navigating the Cisco ASA Series Documentation(Cisco ASA Series 문서 탐색)에서 사용 중인 소프트웨어 버전에 대해 사용 가능한 문서를 참조하십시오.

의 ASA 및 FXOS CLI 액세스

ASACLI를 사용해 문제를 해결하거나 ASDM을 사용하는 대신 ASA를 구성할 수 있습니다. 콘솔 포트에 연결하여 CLI에 액세스할 수 있습니다. 나중에 어떤 인터페이스에서도 ASA로 SSH 액세스를 구성할 수 있습니다. 자세한 내용은 ASA일반 작업 구성 가이드를 참조하십시오.

문제 해결을 위해 ASA CLI에서 FXOS CLI에 액세스할 수 있습니다.

프로시저

단계 1 관리 컴퓨터를 콘솔 포트에 연결합니다. 운영 체제에 필요한 모든 시리얼 드라이버를 설치해야 합니다. 다음 시리얼 설정을 사용하십시오.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

ASA CLI에 연결합니다. 기본적으로 콘솔 액세스에는 사용자 자격 증명이 필요하지 않습니다.

단계 2 특권 EXEC 모드에 액세스합니다.

enable

enable 명령을 처음 입력하면 비밀번호를 변경하라는 메시지가 표시됩니다.

예제:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

ASA에서 설정한 활성화 비밀번호는 ASA가 부팅하는 데 실패하는 경우 FXOS 페일세이프 모드에 진입하는 FXOS **admin** 사용자 비밀번호와 동일합니다.

모든 비 컨피그레이션 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 컨피그레이션 모드를 입력할 수도 있습니다.

특권 모드를 종료하려면 **disable**, **exit**, **quit** 명령을 입력합니다.

단계 **3** 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

예제:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

전역 구성 모드에서 ASA 구성을 시작할 수 있습니다. 전역 구성 모드를 종료하려면 **exit**, **quit** 또는 **end** 명령을 입력합니다.

단계 **4** (선택 사항) FXOS CLI에 연결합니다.

connect fxos [**admin**]

- **admin**—관리자 레벨 액세스를 제공합니다. 이 옵션을 사용하지 않으면 사용자에게는 읽기 전용 권한만 있습니다. 관리 모드에서도 구성 명령은 사용할 수 없습니다.

사용자 자격 증명 관련 프롬프트를 표시하지 않습니다. 현재 ASA 사용자 이름이 FXOS로 전달되며 추가 로그인이 필요하지 않습니다. ASA CLI로 돌아가려면 **exit**을 입력하거나 **Ctrl-Shift-6**, **x**를 입력합니다.

FXOS 내에서 **scope security/show audit-logs** 명령을 사용하여 사용자 활동을 볼 수 있습니다.

예제:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

다음 단계는 무엇입니까?

- ASA를 계속 구성하려면 Navigating the Cisco ASA Series Documentation에서 사용 중인 소프트웨어 버전에 대해 사용 가능한 설명서를 참조하십시오.
- 문제 해결에 대한 자세한 내용은 FXOS 문제 해결 가이드를 참조하십시오.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.