디바이스 및 서비스 온보딩

라이브 디바이스와 모델 디바이스를 모두 CDO에 온보딩할 수 있습니다. 모델 디바이스는 CDO를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 보안 디바이스 커넥터가 CDO를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 SDC(Secure Device Connector)의 내용을 참조하십시오.

이 장에는 다음 섹션이 포함되어 있습니다.

ASA 디바이스 온보딩

이 절차를 사용하여 ASA 모델이 아닌 단일 라이브 ASA 디바이스를 CDO에 온보딩합니다. 여러 ASA를 한 번에 온보딩하려면 대량 ASA 온보딩을 참조하십시오.

Before you begin

디바이스 사전 요건

- 매니지드 디바이스에 Cisco Defense Orchestrator 연결를 검토합니다.

- ASA의 실행 중인 구성 파일은 4.5MB 미만이어야 합니다. 실행 중인 구성 파일의 크기를 확인하려면 ASA 실행 중인 구성 크기 확인을 참조하십시오.
- IP 주소 지정: 각 ASA, ASAv 또는 ASA 보안 상황에는 고유한 IP 주소가 있어야 하며 SDC는 관리 트래픽을 수신하도록 구성된 인터페이스에서 해당 상황에 연결해야 합니다.

인증서 사전 요건

ASA 디바이스에 호환되는 인증서가 없는 경우 디바이스 온보딩이 실패할 수 있습니다. 다음 요구 사항이 충족되었는지 확인하십시오.

- 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
- 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
- 인증서는 SHA-256 인증서여야 합니다. SHA1 인증서는 허용되지 않습니다.
- 다음 조건 중 하나가 참입니다.
  - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
  - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

온보딩 프로세스 중에 인증서 오류가 발생하는 경우 인증서 오류로 인해 ASA를 온보딩할 수 없음에서 자세한 내용을 참조하십시오.

개방형 **SSL** 암호 사전 요건

디바이스에 호환되는 SSL 암호 그룹이 없으면 디바이스는 SDC(Secure Device Connector)와 성공적으로 통신할 수 없습니다. 다음 암호 그룹 중 하나를 사용합니다.

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA에서 사용하는 암호 그룹이 이 목록에 없는 경우 SDC가 이를 지원하지 않으므로 ASA에서 암호 그룹을 업데이트해야 합니다.

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 파란색 더하기 버튼을  클릭하여 ASA를 온보딩합니다.

단계 **3** **ASA** 타일을 클릭합니다.

단계 **4** 디바이스 찾기 단계에서 다음을 수행합니다.

a. **Secure Device Connector(**보안 디바이스 커넥터**)** 버튼을 클릭하고 네트워크에 설치된 보안 디바이스 커넥터를 선택합니다. SDC를 사용하지 않으려는 경우 CDO는 클라우드 커넥터를 사용하여 ASA에 연결할 수 있습니다. 선택은 CDO를 매니지드 디바이스에 연결하는 방법에 따라 달라집니다.

b. 디바이스에 이름을 지정합니다.

c. 디바이스 또는 서비스의 위치(IP 주소, FQDN 또는 URL)를 입력합니다. 기본 포트는 443입니다.

d. **Next(**다음**)**를 클릭합니다.

단계 **5** **Credentials(**자격 증명**)** 단계에서 CDO가 디바이스에 연결하는 데 사용할 ASA 관리자 또는 이와 유사한 최고 권한의 ASA 사용자의 사용자 이름 및 비밀번호를 입력하고 **Next(**다음**)**를 클릭합니다.

단계 **6** (선택 사항) 완료 단계에서 디바이스의 레이블을 입력합니다. 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다. 자세한 내용은 레이블 및 레이블 그룹을 참조하십시오.

단계 **7** 디바이스 또는 서비스에 레이블을 지정한 후에는 **Inventory(**재고 목록**)** 목록에서 볼 수 있습니다.

Note 구성의 크기 및 다른 디바이스 또는 서비스의 수에 따라 구성을 분석하는 데 시간이 걸릴 수 있습니다.

고가용성 쌍의 일부인 **ASA** 온보딩

고가용성 쌍의 일부인 ASA를 온보딩하는 경우 쌍의 기본 디바이스만 온보딩하는 데 ASA 디바이스 온보딩, on page 1를 사용합니다.

다중 상황 모드에서 **ASA** 온보딩

멀티컨텍스트 모드 정보

물리적 어플라이언스에 설치된 단일 ASA를 상황이라고 하는 여러 논리적 디바이스로 분할할 수 있습니다. 다중 상황 모드에서 구성된 ASA에는 다음과 같은 세 가지 구성이 사용됩니다.

- 보안 상황
- 관리 상황

- 시스템 구성

보안 상황 정보

각 보안 상황은 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스의 역할을 합니다. 다중 보안 상황은 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 보안 상황은 프라이빗 클라우드 인프라에 설치된 가상 머신 이미지와 같은 가상 ASA가 아닙니다. 보안 상황은 하드웨어 어플라이언스에 설치된 ASA에 구성됩니다. 각 상황은 해당 어플라이언스의 물리적 인터페이스에 구성됩니다.

다중 상황 모드에 대한 자세한 내용은 ASA CLI 및 ASDM 구성 가이드를 참조하십시오.

CDO는 각 보안 상황을 별도의 ASA로 온보딩하고 별도의 ASA인 것처럼 관리합니다.

관리 상황 정보

관리 상황은 보안 상황과 비슷하지만, 사용자가 관리 상황에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 상황에 액세스할 수 있다는 점이 다릅니다. 관리 상황은 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 상황에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 상황 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다.

CDO는 각 관리 상황을 별도의 ASA로 온보딩하고 별도의 ASA인 것처럼 관리합니다. 또한 CDO는 어플라이언스에서 ASA 및 ASDM 소프트웨어를 업그레이드할 때 관리 상황을 사용합니다.

시스템 구성 관련 정보

시스템 관리자는 시스템 구성에서 각 상황 컨피그레이션 위치, 할당된 인터페이스, 기타 상황 운영 매개 변수를 컨피그레이션함으로써 상황을 추가하고 관리합니다. 이는 단일 모드 컨피그레이션처럼 시작 컨피그레이션이 됩니다. 시스템 구성은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 구성은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 상황 다운로드) 관리 상황으로 지정된 상황 중 하나를 사용합니다.

CDO는 시스템 구성을 온보딩하지 않습니다.

보안 및 관리 상황에 대한 온보딩 사전 요건

보안 및 관리 상황 온보딩에 대한 사전 요건은 다른 ASA의 온보딩에서도 동일합니다. 사전 요건 목록은 ASA 디바이스 온보딩, 1 페이지의 내용을 참조하십시오.

다중 상황 모드에서 ASA를 지원하는 Cisco 어플라이언스를 알아보려면 실행 중인 ASA 소프트웨어 버전에 대한 *CLI 설명서 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드*의 "다중 상황 모드" 장을 참조하십시오.

단일 상황 방화벽으로 실행되는 ASA와 다중 상황 방화벽의 관리 상황에서는 ASDM 및 CDO 액세스에 여러 포트 번호를 사용할 수 있습니다. 그러나 보안 상황의 경우 ASDM 및 CDO 액세스 포트는 포트 443으로 고정됩니다. 이는 ASA의 제한 사항입니다.

온보딩 **ASA** 보안 및 관리 상황

보안 상황 또는 관리 상황을 온보딩하는 방법은 다른 ASA를 온보딩하는 방법과 동일합니다. 온보딩 지침은 ASA 디바이스 온보딩, 1 페이지 또는 대량 ASA 온보딩, 5 페이지의 내용을 참조하십시오.

보안 상황 업그레이드

CDO는 다중 상황 ASA의 각 보안 및 관리 상황을 별도의 ASA로 취급하며, 각각은 개별적으로 온보딩됩니다. 그러나 다중 상황 ASA의 모든 보안 및 관리 상황은 어플라이언스에 설치된 동일한 버전의 ASA 소프트웨어를 실행합니다.

ASA의 보안 상황에서 사용하는 ASA 및 ASDM 버전을 업그레이드하려면 관리 상황을 온보딩하고 해당 상황에서 업그레이드를 수행합니다. 자세한 내용은 단일 ASA에서 ASA 및 ASDM 이미지 업그레이드, 13 페이지 또는 ASA 및 ASDM 대량 업그레이드, 10 페이지 ASA 및 ASDM 대량 업그레이드, 10 페이지의 내용을 참조하십시오.

대량 **ASA** 온보딩

CDO(Cisco Defense Orchestrator)를 사용하면 a.csv 파일에서 모든 ASA에 필요한 정보를 제공하여 ASA를 대량 온보딩할 수 있습니다. ASA가 온보딩되는 동안 필터 창을 사용하여 대기열에 있는 온보딩 시도, 로드 중, 완료 또는 실패한 온보딩 시도를 표시할 수 있습니다.

Before you begin

- 매니지드 디바이스에 Cisco Defense Orchestrator 연결를 검토합니다.
- 온보딩하려는 ASA의 연결 정보가 포함된 .csv 파일을 준비합니다. 한 줄의 ASA에 대한 정보를 추가합니다. 줄의 시작 부분에 #을 사용하여 코멘트를 나타낼 수 있습니다.
  - ASA 위치(IP 주소 또는 FQDN)
  - ASA 관리자 사용자 이름
  - ASA 관리자 비밀번호
  - (선택 사항) CDO의 디바이스 이름
  - SDCName 필드에 CDO를 ASA에 연결하는 데 사용할 네트워크의 SDC(Secure Device Connector) 이름을 지정합니다. SDC를 사용하여 ASA를 CDO에 연결하지 않으려는 경우에도 "none"을 입력할 수 있습니다. 디바이스를 온보딩할 때 SDCName 필드에 "none"을 지정하면 클라우드 커넥터를 사용하여 ASA를 온보딩합니다. 클라우드 커넥터를 사용하면 SDC를 설치하지 않고도 디바이스를 CDO에 연결할 수 있습니다. 선택은 CDO를 매니지드 디바이스에 연결하는 방법에 따라 달라집니다.
  - (선택 사항) CDO용 디바이스 레이블
  - 하나의 레이블을 추가하려면 마지막 CSV 필드에 레이블 이름을 추가합니다.
  - 디바이스에 둘 이상의 레이블을 추가하려면 값을 따옴표로 묶습니다. 예: 알파, 베타, 감마.

- 범주 및 선택 항목 레이블을 추가하려면 콜론(:)으로 두 값을 구분합니다. 예를 들면 `Rack:50` 입니다.

구성 파일의 샘플:

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

Caution CDO는 .csv 파일의 데이터를 검증하지 않습니다. 항목의 정확성을 확인해야 합니다.

단계 **1** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 파란색 더하기 버튼 을 클릭하여 ASA를 온보딩합니다.

단계 **3** Onboarding(온보딩) 페이지에서 **Multiple ASAs(**여러 **ASA)** 타일을 클릭합니다.

단계 **4** **Browse(**찾아보기**)**를 클릭하여 ASA 항목이 포함된 .csv 파일을 찾습니다. 지정한 디바이스가 이제 ASA 대량 온보딩 테이블에 대기되어 온보딩할 준비가 되었습니다.

Caution 온보딩 프로세스가 완료될 때까지 ASA 대량 온보딩 페이지에서 다른 곳으로 이동하지 마십시오. 다른 곳으로 이동하면 온보딩 프로세스가 중지됩니다.

단계 **5** **Start(**시작**)**를 클릭합니다. ASA 대량 온보딩 테이블의 상태 열에서 온보딩 프로세스의 진행 상황을 확인할 수 있습니다. 디바이스가 성공적으로 온보딩되면 상태가 "Complete(완료)"로 변경됩니다.

What to do next

대량 온보딩을 일시 중지하고 나중에 다시 시작해야 하는 경우 대량 온보딩 일시 중지 및 다시 시작, on page 6의 내용을 참조하십시오.

.

대량 온보딩 일시 중지 및 다시 시작

온보딩 프로세스를 일시 중지해야 하는 경우 **Pause(**일시 중지**)**를 클릭합니다. CDO가 온보딩을 시작한 모든 디바이스의 온보딩을 완료합니다. 벌크 온보딩 프로세스를 재개하려면 **Start(**시작**)**를 클릭합니다. CDO가 대기 중인 다음 디바이스의 온보딩을 시작합니다.

Pause(일시 중지**)**를 클릭하고 이 페이지에서 나가면 페이지로 돌아가 처음부터 대량 온보딩 절차를 다시 수행해야 합니다. 그러나 CDO는 이미 온보딩한 디바이스를 인식하고, 이 새 온보딩 시도의 디바이스를 중복으로 표시하며, 목록을 빠르게 이동하여 대기열에 있는 디바이스를 온보딩합니다.

ASA 모델 생성 및 가져오기

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.
단계 3 **ASA** 탭을 클릭합니다.
단계 4 ASA 디바이스를 선택하고 왼쪽 창의 **Management(**관리**)**에서 **Configuration(**구성**)**을 클릭합니다.
단계 5 **Download(**다운로드**)**를 클릭하여 디바이스 컨피그레이션을 로컬 컴퓨터에 다운로드합니다.

ASA 구성 가져오기

주의: ASA의 실행 중인 구성 파일은 4.5MB 미만이어야 합니다. 온보딩하기 전에 구성 파일의 크기를 확인합니다.

단계 1 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.
단계 2 파란색 더하기() 버튼을 클릭하여 구성을 가져옵니다.
단계 3 오프라인 관리를 위해 구성 가져오기를 클릭합니다.
단계 4 **Device Type(**장치 유형**)**을 **ASA**로 선택합니다.
단계 5 **Browse(**찾아보기**)**를 클릭하고 업로드할 구성 파일(텍스트 형식)을 선택합니다.
단계 6 구성이 확인되면 디바이스 또는 서비스에 레이블을 지정하라는 메시지가 표시됩니다. 자세한 내용은 레이블 및 레이블 그룹을 참조하십시오.
단계 7 모델 디바이스에 레이블을 지정한 후에는 **Devices & Services(**디바이스 및 서비스**)** 목록에서 볼 수 있습니다.

Note 구성의 크기 및 다른 디바이스 또는 서비스의 수에 따라 구성을 분석하는 데 시간이 걸릴 수 있습니다.

CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

단계 1 CDO에 로그인합니다.
단계 2 **Inventory(**인벤토리**)** 페이지로 이동합니다.
단계 3 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.
단계 4 오른쪽에 있는 디바이스 작업 패널에서 **Remove(**제거**)**를 선택합니다.

단계 **5** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(**취소**)**을 선택합니다.

오프라인 관리를 위한 디바이스 컨피그레이션 가져오기

오프라인 관리를 위해 디바이스의 구성을 가져오면 네트워크의 라이브 디바이스에서 작업하지 않고도 디바이스의 구성을 검토하고 최적화할 수 있습니다. CDO는 이러한 업로드된 구성 파일을 "모델"이라고도 합니다.

이러한 디바이스의 구성을 CDO로 가져올 수 있습니다.

- ASA(Adaptive Security Appliance) ASA 모델 생성 및 가져오기를 참조하십시오.
- FTD(Firepower Threat Defense)
- ASR(Aggregation Services Router) 및 ISR(Integrated Services Router)과 같은 Cisco IOS 디바이스

ASA 및 ASDM 업그레이드 사전 요건

CDO(Cisco Defense Orchestrator)는 개별 ASA, 여러 ASA, 액티브-스탠바이 구성의 ASA, 단일 상황 또는 다중 상황 모드에서 실행 중인 ASA에 설치된 ASA 및 ASDM 이미지를 업그레이드하는 데 도움이 되는 마법사를 제공합니다.

CDO는 업그레이드할 수 있는 ASA 및 ASDM 이미지의 저장소를 유지 관리합니다. CDO의 이미지 저장소에서 업그레이드 이미지를 선택하면 CDO는 백그라운드에서 필요한 모든 업그레이드 단계를 수행합니다. 마법사는 호환 가능한 ASA 소프트웨어 및 ASDM 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Cisco에서는 CDO에서 선택한 이미지가 ASA에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다. CDO는 주기적으로 ASA 이진 파일의 재고 목록을 검토하고 최신 ASA 및 ASDM 이미지가 있으면 해당 이미지를 저장소에 추가합니다. 이는 ASA에서 인터넷에 대한 아웃바운드 액세스 권한이 있는 고객에게 가장 적합한 옵션입니다.

CDO의 이미지 저장소에는 일반적으로 사용 가능한(GA) 이미지만 포함됩니다. 목록에 특정 GA 이미지가 표시되지 않으면 Cisco TAC에 문의하거나 지원 문의 페이지에서 지원팀에 이메일을 보내십시오. 설정된 지원 티켓 SLA를 사용하여 요청을 처리하고 누락된 GA 이미지를 업로드합니다.

ASA에서 인터넷에 대한 아웃바운드 액세스 권한이 없는 경우 Cisco.com에서 원하는 ASA 및 ASDM 이미지를 다운로드하여 자체 저장소에 저장하고 업그레이드 마법사에 해당 이미지에 대한 맞춤형 URL을 제공하면 CDO가 이러한 이미지를 사용하여 업그레이드를 수행합니다. 그러나 이 경우 업그레이드 대상 이미지를 결정합니다. CDO는 이미지 무결성 검사 또는 디스크 공간 검사를 수행하지 않습니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다.

모든 **ASA**에 대한 구성 사전 요건

- ASA에서 DNS를 활성화해야 합니다.
- CDO의 이미지 저장소에서 업그레이드 이미지를 사용하는 경우 ASA에서 인터넷에 연결할 수 있어야 합니다.
- ASA와 저장소 FQDN 간의 HTTPS 연결을 확인합니다.
- ASA가 CDO에 성공적으로 온보딩되었습니다.
- ASA가 CDO에 동기화됩니다.
- ASA가 온라인 상태입니다.
- 맞춤형 URL 업그레이드의 경우:
  - Cisco ASA 업그레이드 가이드를 사용하여 ASA와 호환되는 ASA 및 ASDM 버전을 확인합니다.
  - 이미지 저장소에 ASA 및 ASDM 이미지를 다운로드합니다.
  - ASA에서 이미지 저장소에 액세스할 수 있는지 확인합니다.
  - ASA 및 ASDM 이미지를 저장할 충분한 디스크 공간이 ASA에 있는지 확인합니다.
  - URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

Firepower 1000 및 **Firepower 2100 Series** 디바이스에 대한 구성 사전 요건

- Firepower 2100 Series 디바이스의 FXOS 모드는 어플라이언스 모드로 구성되어야 합니다. 자세한 내용은 Firepower 2100을 어플라이언스 또는 플랫폼 모드로 설정을 참조하십시오.
- 디바이스에서 ASA 버전 9.13(1) 이상을 실행해야 합니다.
- ASA 소프트웨어를 업그레이드하기 전에 FXOS 번들을 업그레이드해야 합니다. 자세한 내용은 Firepower 2100 ASA 및 FXOS 호환성을 참조하십시오.

ASA를 실행하는 **Firepower 4100** 및 **Firepower 9300 Series** 디바이스

CDO는 Firepower 4100또는 Firepower 9300 Series 디바이스에 대한 업그레이드를 지원하지 않습니다. 이러한 디바이스는 CDO 외부에서 업그레이드해야 합니다.

업그레이드 지침

- CDO는 액티브/스탠바이 "페일오버" 쌍으로 구성된 ASA를 업그레이드할 수 있습니다. CDO는 액티브/액티브 "클러스터링된" 쌍으로 구성된 ASA를 업그레이드할 수 없습니다.

소프트웨어 및 하드웨어 사전 요건

업그레이드할 수 있는 최소 ASA 및 ASDM 버전:

- ASA: ASA 9.1.2
- ASDM: 최소 버전이 없습니다.

지원되는 하드웨어 버전

- ASA 소프트웨어 및 하드웨어 지원을 참조하십시오.

ASA 및 ASDM 대량 업그레이드

단계 **1** ASA 및 ASDM 이미지 업그레이드에 대한 업그레이드 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.

Note ASA 1000 또는 2000 Series 디바이스를 업그레이드하는 경우 ASA 및 ASDM 업그레이드 사전 요건을 읽어보십시오.

단계 **2** (선택 사항) 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭하고 변경 로그에서 이 작업에 의해 업그레이드된 디바이스를 식별하는 변경 요청 레이블을 생성합니다.

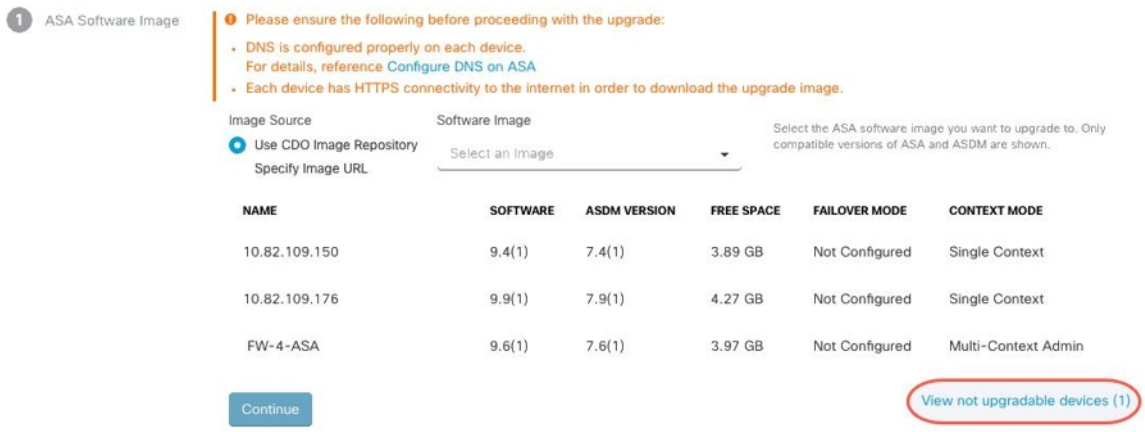
단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 필터를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.

단계 **5** 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.

단계 **6** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **7** Bulk Device Upgrade(대량 디바이스 업그레이드) 페이지에 업그레이드할 수 있는 디바이스가 표시됩니다. 선택한 디바이스 중 업그레이드할 수 없는 디바이스가 있으면 CDO에서 업그레이드할 수 없는 디바이스를 볼 수 있는 링크를 제공합니다.



단계 **8** 1단계에서 **Use CDO Image Repository(CDO** 이미지 저장소 사용**)**를 클릭하여 업그레이드할 ASA 소프트웨어 이미지를 선택하고 **Continue(**계속**)**를 클릭합니다.

이 목록에는 선택한 소프트웨어 버전으로 업그레이드할 수 있는 ASA의 수가 표시됩니다. 아래 예에서는 모든 디바이스를 버전 9.9(1.2)로 업그레이드할 수 있으며, 두 개의 디바이스를 9.8(2)로 업그레이드할 수 있으며, 디바이스 중 하나를 9.6(1)으로 업그레이드할 수 있습니다.

선택한 소프트웨어 버전이 선택한 디바이스와 호환되지 않는 경우 CDO에서 알림을 보냅니다. 아래 예에서 CDO는 10.82.109.176 디바이스를 이미 실행 중인 것보다 이전 버전으로 업그레이드할 수 없습니다.

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
✔ 10.82.109.150	9.4(1)	7.4(1)	3.89 GB	Not Configured	Single Context
✔ FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin
✖ 10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context

단계 **9** 2단계에서 업그레이드할 ASDM 이미지를 선택합니다. 업그레이드할 수 있는 ASA와 호환되는 ASDM 선택 항목만 표시됩니다.

단계 **10** 3단계에서는 선택 사항을 확인하고 ASA에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

단계 **11** 준비가 되면 **Perform Upgrade(**업그레이드 수행**)**를 클릭합니다.

Note 업그레이드가 실패하면 CDO에 메시지가 표시됩니다. 업그레이드 실패의 원인은 ASA 및 ASDM 이미지를 ASA로 전송하지 못하는 네트워크 문제인 경우가 많습니다.

단계 **12** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 Schedule Upgrade(업그레이드 예약) 버튼을 클릭합니다.

단계 **13** (다중 상황 모드의 경우) 관리자 상황 및 보안 상황이 부팅된 후 보안 상황에 "새 인증서가 탐지되었습니다."라는 메시지가 표시될 수 있습니다. 이 메시지가 표시되면 모든 보안 상황에 대한 인증서를 수락합니다. 업그레이드로 인한 기타 변경 사항을 수락합니다.

단계 **14** 알림 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 Jobs(작업) 페이지로 이동합니다.

단계 **15** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

자체 저장소의 이미지를 사용하여 여러 **ASA** 업그레이드

단계 **1** ASA 및 ASDM 이미지 업그레이드에 대한 업그레이드 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.

단계 **2** (선택 사항) 탐색 모음에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭하고 변경 로그에서 이 작업에 의해 업그레이드된 디바이스를 식별하는 change request labe(변경 요청 레이블)을 생성합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

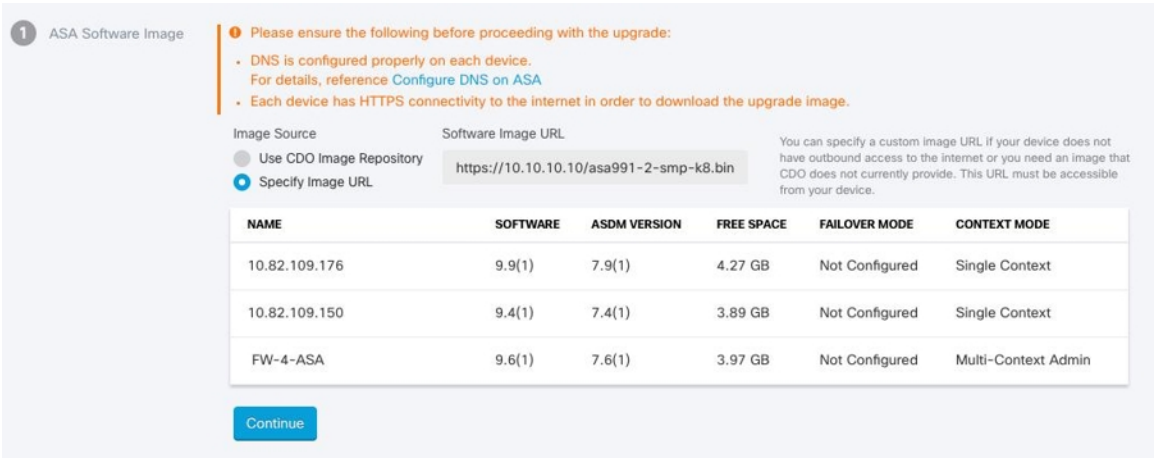
단계 **4** 필터를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.

단계 **5** 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.

단계 **6** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **7** 1단계에서 **Specify Image URL(**이미지 **URL** 지정**)**을 클릭하고 **Software Image URL(**소프트웨어 이미지 **URL)** 필드에 업그레이드할 ASA 이미지의 URL을 입력한 후 **Continue(**계속**)**를 클릭합니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

Note 아래 그림은 소프트웨어 이미지 URL 필드의 HTTPS URL을 보여줍니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.



단계 **8** 2단계에서 **Specify Image URL(**이미지 **URL** 지정**)**을 클릭하고 **Software Image URL(**소프트웨어 이미지 **URL)** 필드에 업그레이드할 ASDM 이미지의 URL을 입력한 후 **Continue(**계속**)**를 클릭합니다.

단계 **9** 3단계에서는 선택 사항을 확인하고 ASA에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

단계 **10** 준비가 되면 **Perform Upgrade(**업그레이드 수행**)**를 클릭합니다.

Note 업그레이드가 실패하면 CDO에 메시지가 표시됩니다. 업그레이드 실패의 원인은 ASA 및 ASDM 이미지를 ASA로 전송하지 못하는 네트워크 문제인 경우가 많습니다.

단계 **11** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 Schedule Upgrade(업그레이드 예약) 버튼을 클릭합니다.

단계 **12** (다중 상황 모드의 경우) 관리자 상황 및 보안 상황이 부팅된 후 보안 상황에 "새 인증서가 탐지되었습니다."라는 메시지가 표시될 수 있습니다. 이 메시지가 표시되면 모든 보안 상황에 대한 인증서를 수락합니다. 업그레이드로 인한 기타 변경 사항을 수락합니다.

단계 **13** 알림 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 Jobs(작업) 페이지로 이동합니다.

단계 **14** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

What to do next

업그레이드 참고 사항

- Devices & Services(디바이스 및 서비스) 페이지를 열고 테이블의 Configuration Status(구성 상태) 열을 확인하여 업그레이드 배치의 진행 상황을 모니터링할 수도 있습니다.
- Devices & Services(디바이스 및 서비스) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 대량 업그레이드에 포함된 단일 디바이스의 진행 상황을 볼 수 있습니다. CDO에서 해당 디바이스의 Device Upgrade(디바이스 업그레이드) 페이지로 이동합니다.

단일 ASA에서 ASA 및 ASDM 이미지 업그레이드

단일 ASA에서 ASA 및 ASDM 이미지를 업그레이드하려면 다음 절차를 따르십시오.

단계 **1** ASA 및 ASDM 이미지 업그레이드에 대한 업그레이드 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.

Note ASA 1000 또는 2000 Series 디바이스를 업그레이드하는 경우 ASA 및 ASDM 업그레이드 사전 요건을 읽어보십시오.

단계 **2** 내비게이션 바에서 **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** (선택 사항) 변경 로그에서 이 작업에 의해 업그레이드된 디바이스를 식별하는 변경 요청 레이블을 생성합니다.

단계 **5** 업그레이드할 디바이스를 선택합니다.

단계 **6** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **7** Device Upgrade(디바이스 업그레이드) 페이지에서 마법사가 제공하는 지침을 따릅니다.

a. 1단계에서 **Use CDO Image Repository(CDO** 이미지 저장소 사용**)**를 클릭하여 업그레이드할 ASA 소프트웨어 이미지를 선택하고 **Continue(**계속**)**를 클릭합니다.

Note ASA 및 ASDM을 자체 저장소에 저장된 이미지로 업그레이드하는 경우 **Specify Image URL(**이미지 **URL** 지정**)**을 선택하고 Software Image URL(소프트웨어 이미지 URL) 필드에 ASA 또는 ASDM 이미지의 URL을 입력합니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

(선택 사항) CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade(**업그레이드 예약**)**를 클릭합니다.

b. 2단계에서 업그레이드할 ASDM 이미지를 선택합니다. 업그레이드할 수 있는 ASA와 호환되는 ASDM 선택 항목만 표시됩니다.

c. 3단계에서는 선택 사항을 확인하고 ASA에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

단계 **8** 준비가 되면 **Perform Upgrade(**업그레이드 수행**)**를 클릭합니다.

단계 **9** (다중 상황 모드의 경우) 관리자 상황 및 보안 상황이 부팅된 후 보안 상황에 "새 인증서가 탐지되었습니다."라는 메시지가 표시될 수 있습니다. 이 메시지가 표시되면 모든 보안 상황에 대한 인증서를 수락합니다. 업그레이드로 인한 기타 변경 사항을 수락합니다. 데모를 보고 싶으십니까? 이 절차의 스크린캐스트를 시청하십시오!

What to do next

업그레이드 참고 사항

- 업그레이드할 이미지를 선택하고 마음이 바뀌면 소프트웨어 이미지와 연결된 **Skip Upgrade(**업그레이드 건너뛰기**)** 확인란을 선택합니다. 이미지가 디바이스에 복사되지 않으며 디바이스가 이미지와 함께 업그레이드되지도 않습니다.
- **Perform Upgrade(**업그레이드 수행**)** 단계에서 ASA에 이미지를 복사하기만 하려는 경우 나중에 Device Upgrade(디바이스 업그레이드) 페이지로 돌아가 "Upgrade Now(지금 업그레이드)"를 클릭하여 업그레이드를 수행할 수 있습니다. 복사 작업이 완료되면 Devices & Services(디바이스 및 서비스) 페이지에 해당 디바이스에 대한 "Ready to Upgrade(업그레이드 준비 완료)" 메시지가 표시됩니다.
- 이미지를 복사하고 설치하고 디바이스를 재부팅하는 동안에는 디바이스에서 작업을 수행할 수 없습니다. 이미지를 설치한 다음 재부팅하는 디바이스는 Devices & Services(디바이스 및 서비스) 페이지에 "Upgrading(업그레이드)"으로 표시됩니다.
- 업그레이드 프로세스 중에는 디바이스에서 작업을 수행할 수 없습니다. 즉, 이미지를 설치하고 디바이스를 재부팅합니다.
- 이미지를 디바이스에 복사하기만 선택한 경우 디바이스에서 작업을 수행할 수 있습니다. 이미지를 복사하는 디바이스는 Devices & Services(디바이스 및 서비스) 페이지에 "Copying Images(이미지 복사 중)"로 표시됩니다.
- 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 새 인증서 탐지를 참조하십시오.

액티브/스탠바이 쌍의 **ASA** 및 **ASDM** 이미지 업그레이드

액티브/스탠바이 페일오버 모드에서 ASA 쌍을 업그레이드하기 전에 아래의 사전 요건을 검토하십시오. ASA를 구성하고 페일오버 모드에서 작동하는 방법에 대한 자세한 내용은 ASA 설명서에서 고가용성을 위한 페일오버를 참조하십시오.

데모를 보고 싶으십니까? 이 절차의 스크린캐스트를 시청하십시오.

사전 요건

- ASA 및 ASDM 이미지 업그레이드에 대한 요구 사항 및 중요 정보는 ASA 및 ASDM 업그레이드 사전 요건을 검토하십시오.
- 기본(액티브) 및 보조(스탠바이) ASA는 액티브/스탠바이 페일오버 모드에서 구성됩니다.
- 기본 ASA는 액티브/스탠바이 쌍의 액티브 디바이스입니다. 기본 ASA가 비활성 상태인 경우 CDO는 업그레이드를 수행하지 않습니다.
- 기본 및 보조 ASA 소프트웨어 버전은 동일합니다.

워크플로

이 프로세스에서는 CDO가 ASA의 활성/대기 쌍을 업그레이드합니다.

단계 **1** CDO는 ASA 및 ASDM 이미지를 두 ASA에 모두 다운로드합니다.

Note 사용자는 ASA 및 ASDM 이미지를 다운로드할 수 있지만, 바로 업그레이드할 수는 없습니다. ASA 및 ASDM 이미지를 이전에 다운로드한 경우 CDO는 해당 이미지를 다시 다운로드하지 않습니다. CDO는 이 다음 단계로 업그레이드 워크플로를 계속 진행합니다.

단계 **2** CDO는 보조 ASA를 먼저 업그레이드합니다.

단계 **3** 업그레이드가 완료되고 보조 ASA가 "Standby-Ready(대기 준비)" 상태로 돌아가면 CDO에서 페일오버를 시작하여 보조 ASA가 활성 ASA가 되도록 합니다.

단계 **4** CDO는 현재 대기 ASA인 기본 ASA를 업그레이드합니다.

단계 **5** 기본 ASA가 "Standby-Ready(대기 준비)" 상태로 돌아가면 CDO가 페일오버를 시작하여 기본 ASA가 활성 ASA가 되도록 합니다.

Warning 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 새 인증서 탐지를 참조하십시오.

액티브/스탠바이 쌍의 **ASA** 및 **ASDM** 이미지 업그레이드

단계 **1** CDO에 로그인합니다.

단계 **2** **Devices & Services(**디바이스 및 서비스**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 업그레이드할 디바이스를 선택합니다.

단계 **5** **Device Actions(**디바이스 작업**)** 창에서 **Upgrade(**업그레이드**)**를 클릭합니다.

디바이스의 장애 조치 모드는 Active/Standby(활성/대기)입니다.

단계 **6** Device Upgrade(디바이스 업그레이드) 페이지에서 마법사가 제공하는 지침을 따릅니다.

Note ASA 및 ASDM을 자체 저장소에 저장된 이미지로 업그레이드하는 경우 **Specify Image URL(**이미지 **URL** 지정**)**을 선택하고 Software Image URL(소프트웨어 이미지 URL) 필드에 ASA 또는 ASDM 이미지의 URL을 입력합니다. FTP, TFTP, HTTP, HTTPS, SCP 및 SMB 프로토콜 중 하나를 사용하여 저장소에서 이미지를 검색할 수 있습니다. URL 구문 정보는 맞춤형 URL 업그레이드를 참조하십시오.

맞춤형 **URL** 업그레이드

새 ASA 소프트웨어 및 ASDM 이미지로 ASA를 업그레이드하는 경우 CDO(Cisco Defense Orchestrator)에서 이미지 저장소에 저장한 이미지를 사용하거나 자체 이미지 저장소에 저장한 이미지를 사용할 수 있습니다. ASA에 인터넷에 대한 아웃바운드 액세스가 없는 경우, CDO를 사용하여 ASA를 업그레이드하는 가장 좋은 방법은 자체 이미지 저장소를 유지하는 것입니다.

CDO는 ASA의 copy 명령을 사용하여 이미지를 검색하고 ASA의 플래시 드라이브(disk0:/)에 복사합니다. Specify Image URL(이미지 URL 지정) 필드에서 copy 명령의 URL 부분을 제공합니다. 예를 들어 전체 copy 명령은 다음과 같습니다.

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

다음을 제공합니다.

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

Specify Image URL(이미지 URL 지정) 필드에 입력합니다.

CDO는 업그레이드 이미지를 검색하는 http, https, ftp, tftp, smb 및 scp 방법을 지원합니다.

URL 구문 예

다음은 ASA copy 명령에 대한 URL 구문의 예입니다. 이러한 URL 예에서는 다음을 가정합니다.

- 이미지 저장소 주소: 10.10.10.10
- 이미지 저장소에 액세스하기 위한 사용자 이름: admin
- 비밀번호: adminpass
- 경로: images/asa
- 이미지 파일 이름: asa991-smp-k8.bin

http[**s**]**://** [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename*]

https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin

ftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;type=** *xx*]]â€"The **type** 은 **ap**(ASCII 패시브 모드),**an**(ASCII 일반 모드), **ip**(기본 바이너리 패시브 모드), **in**(바이너리 일반 모드)과 같은 키워드 중 하나일 수 있습니다.

ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin

tftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;int=** *interface_name*]]

tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside

Note 경로 이름은 공백을 포함할 수 없습니다. 경로 이름에 공백이 있으면 **copy tftp** 명령 대신 **tftp-server** 명령에서 경로를 설정합니다. **;int=** *interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다.

smb:/[[*path* **/**] *filename*] - UNIX 서버 로컬 파일 시스템을 표시합니다.

smb:/images/asa/asa991-smp-k8.bin

scp:// [[*user* [**:** *password*] **@**] *server* [**/** *path*] **/** *filename* [**;int=** *interface_name*]]â€"The**;int=** *interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다.

scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside
SCP example without a username and password:
scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside

Cisco ASA Series 명령 참조, A~H 명령 가이드의 URL 구문이 포함된 전체 copy 명령.

맞춤형 URL을 사용하여 ASA 및 ASDM 이미지를 업그레이드하는 방법에 대한 자세한 내용은 ASA 및 ASDM 업그레이드 사전 요건을 참조하십시오.