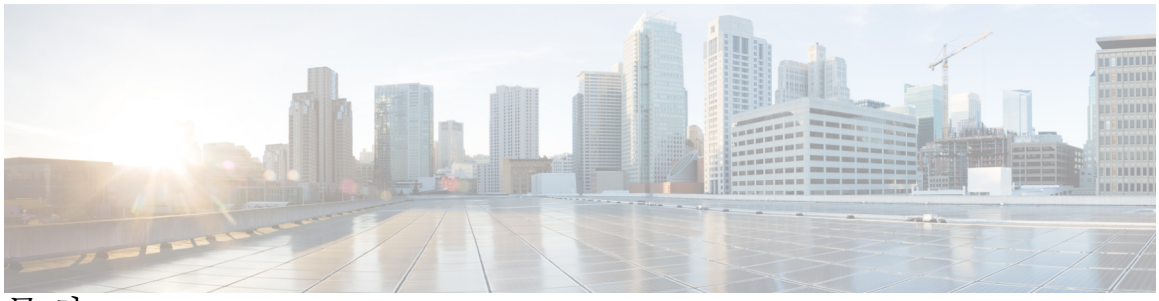
AWS EC2에 Cisco Content Security Virtual Appliances 설치 설명서

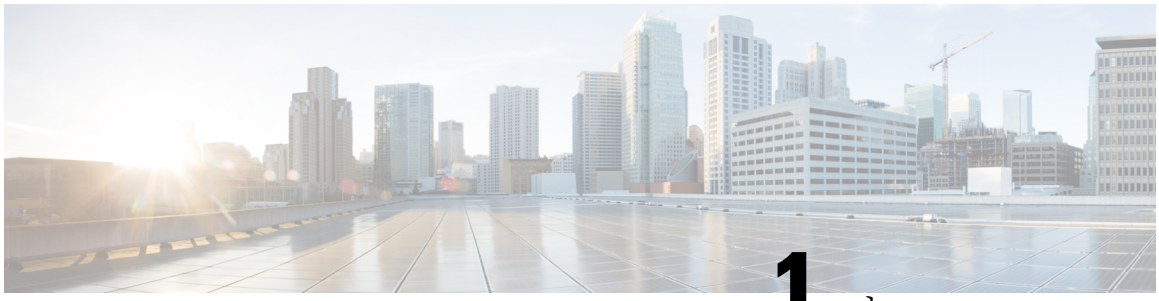
초판: 2023년 2월 20일

최종 변경: 2023년 2월 24일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

Cisco Content Security Virtual Appliance 정보

Cisco Content Security 가상 어플라이언스는 물리적 Secure Email Gateway(이전 명칭은 Email Security Appliance 또는 ESA), Secure Web Appliance(이전 명칭은 Web Security Appliance 또는 WSA) 및 Secure Email and Web Manager(이전 명칭은 Security Management Appliance 또는 SMA)와 동일하게 작동합니다. 몇 가지 사소한 차이가 있으며, 가상 어플라이언스 관리에 설명되어 있습니다.

AWS(Amazon Web Services) EC2(Elastic Compute Cloud) 구축에서 구현하려면 Amazon Marketplace에서 제공되는 AMI(Amazon Machine Images)를 사용합니다.

참고 Cisco Secure Email Gateway, Secure Web, Secure Email and Web Manager 가상 어플라이언스는 AWS EC2에서 지원됩니다.

Amazon Machine Image 정보

AMI(Amazon Machine Image)를 사용하여 EC2 내부에 가상 머신 인스턴스를 생성할 수 있습니다. Secure Web Appliance 및 Secure Email and Web Manager용 AMI는 AWS Marketplace에서 구매할 수 있습니다. Secure Email Gateway는 AWS Marketplace에서 사용할 수 없습니다. AMI 이미지를 프로비저닝하려면 AWS 계정 세부 정보(사용자 이름 및 지역)를 사용하여 Cisco 영업 담당자에게 문의하십시오.

필요한 AMI를 선택하고 구축을 계속 진행합니다.

Cisco Secure Email Gateway, Secure Web 및 Secure Email and Web Manager 가상 어플라이언스 AMI

다음 표에는 Cisco Secure Email Gateway, Secure Web, Secure Email and Web Manager 가상 어플라이언스에 대한 AMI 세부 정보가 나와 있습니다.

Cisco Secure Email Gateway 가상 어플라이언스**(AsyncOS 14.0.0-692)**

Cisco Secure Email Gateway Virtual Appliance용 **AsyncOS** 릴리스	**Virtual Appliance**	**AMI ID**
AsyncOS 14.0.0-692	**C100V**	Cisco Secure Email Virtual Gateway-14-0-0-692-C100V-200421.ami
	C300V	Cisco Secure Email Virtual Gateway-14-0-0-692-C300V-200421.ami
	C600V	Cisco Secure Email Virtual Gateway-14-0-0-692-C600V-200421.ami

Cisco Secure Email 및 **Web Manager Virtual Appliance(AsyncOS 14.0.0-404)** 퍼블릭 **AMI**

콘솔을 사용하여 공유 퍼블릭 AMI를 찾으려면 다음 단계를 수행합니다.

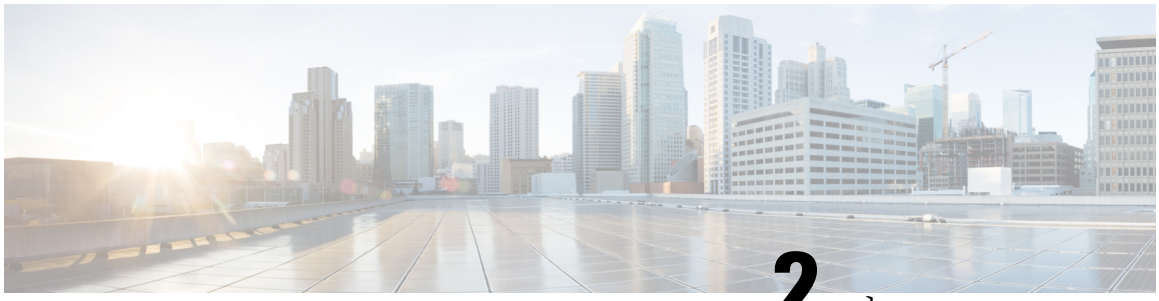
1. Amazon EC2 콘솔을 엽니다.
2. 탐색창에서 **Logon Page(**로그온 페이지**)**를 선택합니다.
3. 첫 번째 필터에서 **Public images(**퍼블릭 이미지**)**를 선택합니다.
4. 검색 창을 선택하고 필요한 가상 어플라이언스 모델에 따라 zeus-14-0-0-404-M600V를 입력합니다.

Cisco Secure Email 및 **Web Manager Virtual Appliance(AsyncOS 14.0.0-404)**	**AMI ID**
M600V	zeus-14-0-0-404-M600V-AMI-230421
M300V	zeus-14-0-0-404-M300V-AMI-230421
M100V	현재 사용 가능한 이미지가 없습니다.

라이선스

기존의 Secure Email Gateway, Secure Web 또는 Secure Email and Web Manager 어플라이언스 라이선스를 Amazon AWS에서 구축하는 데 사용할 수 있습니다. 인스턴스를 구축하고 시작한 후 라이선스를 설치할 수 있습니다. AWS 인프라 요금만 지불하면 됩니다.

기존 고객인 경우 가상 ESA, 가상 WSA 또는 가상 SMA 라이선스에 대한 모범 사례 기술 자료에서 가상 라이선스(VLN) 얻기를 참조하십시오. 신규 고객인 경우 가장 가까운 Cisco 파트너에게 문의하여 라이선스를 받으십시오.



2 장

AWS에 구축

AWS에 구축

참고

- Cisco Secure Email Gateway 온프레미스 어플라이언스는 AWS의 Cisco Secure Email and Web Manager 어플라이언스 구축에서 지원되지 않습니다.

Secure Email Gateway, Secure Web 또는 Secure Email and Web Manager 가상 어플라이언스를 구축하려면 다음 단계를 수행합니다.

	수행해야 할 작업	추가 정보
1단계	EC2에서 인스턴스를 설정하기 전에 사전 요구 사항 작업을 완료하고 필요한 정보를 가져와 환경을 준비해야 합니다.	환경 준비

AWS에 구축

	수행해야 할 작업	추가 정보
2단계	Amazon Marketplace에서 AMI를 선택하고 적절한 인스턴스 유형을 선택합니다. 참고 Secure Email Gateway는 AWS Marketplace에서 사용할 수 없습니다. AMI 이미지를 프로비저닝하려면 AWS 계정 세부 정보(사용자 이름 및 지역)를 사용하여 Cisco 영업 담당자에게 문의하십시오.	가상 어플라이언스 AMI 선택 및 인스턴스 유형 선택.
3단계	인스턴스가 사용 가능하고 필요에 따라 작동하는 데 필요한 네트워크, 서브넷, IP 주소 할당 및 기타 세부 정보를 구성합니다. 참고 하나의 기본 네트워크 인터페이스(관리)가 인스턴스에 자동으로 할당됩니다. 필요한 경우 데이터 인터페이스(S100V의 경우 P1, S300V 및 S600V의 경우 P1, P2)를 생성할 수 있습니다.	인스턴스 세부 정보 구성
4단계	기본 스토리지 설정을 유지하거나 필요에 따라 태그를 구성합니다.	스토리지 구성 및 태그 추가.
5단계	보안 그룹을 구성합니다. 모든 구성 설정을 검토하고 인스턴스를 시작합니다.	보안 그룹 구성, 인스턴스 검토 및 시작.
6단계	어플라이언스에 라이센스를 설치하고 웹 인터페이스가 어플라이언스별 호스트 이름으로 응답하지 않도록 합니다. **hostheader** 명령을 사용하고 변경 사항을 커밋합니다.	시작된 인스턴스 구성.
7단계	어플라이언스의 웹 인터페이스에 연결합니다. 시스템 설정 마법사를 실행하거나, 구성 파일을 업로드하거나, 기능을 구성할 수 있습니다.	어플라이언스의 웹 인터페이스에 연결.
8단계	(선택 사항) 필요한 경우 AWS EC2 Management Console에서 탄력적 IP 주소를 구성합니다.	탄력적 IP 주소 생성.
9단계	어플라이언스에서 라이선스 만료 알림을 구성합니다.	라이선스 만료가 임박했을 때 알림을 보내도록 어플라이언스 구성.

환경 준비

AWS EC2에서 Secure Email Gateway, Secure Web 또는 Secure Email and Web Manager 가상 어플라이언스를 구축하는 데 필요한 리소스와 파일이 있는지 확인합니다. 예를 들면 다음과 같습니다.

- Secure Email Gateway, Secure Web 또는 Secure Email and Web Manager 가상 어플라이언스에 대한 유효한 라이선스.
- Web Security 어플라이언스의 기본 사용자 이름 및 비밀번호:

  — `admin` 및 `ironport`
- EC2 Management Console의 리소스:

  — 인스턴스에 연결할 수 있는 영구 공용 IP 주소가 필요한 경우 사용할 탄력적 IP 주소를 결정하거나 새 주소를 생성합니다. 새 인스턴스를 시작하는 동안 자동으로 할당되는 공용 IP 주소는 동적입니다.

  — 사용할 VPC를 확인하거나 구축에 사용할 VPC를 구성합니다. 기본 VPC를 사용할 수도 있습니다.

  — 관리자와 다른 사용자가 어플라이언스에 액세스하는 방법에 따라 어플라이언스에 할당할 IP 주소의 유형(퍼블릭 또는 프라이빗)을 결정해야 합니다.

  — 사용할 IAM 역할을 확인하거나 구축에 사용할 IAM 역할을 구성합니다.

  — 서브넷을 구성하고 라우팅 테이블에 인터넷 게이트웨이를 가리키는 기본 경로가 있는지 확인합니다.

  — 보안 그룹을 구성하거나 새로 생성합니다.

  — 가상 어플라이언스가 올바르게 통신하기 위해 여는 가장 일반적인 포트는 다음과 같습니다.

    - SSH TCP 22
    - TCP 443
    - TCP 8443
    - TCP 3128
    - (선택 사항) 디버깅을 위한 ICMP(필요한 경우).
- AWS에서 EC2 인스턴스에 등록할 개인 키(PEM 또는 CER 파일)에 액세스할 수 있는지 확인합니다. 가상 어플라이언스 인스턴스를 시작하는 동안 새 개인 키를 생성할 수도 있습니다.

참고 Windows 클라이언트의 경우 PEM 파일에 액세스하려면 SSH 클라이언트가 필요합니다.

가상 어플라이언스 AMI 선택 및 인스턴스 유형 선택

AWS 계정에서 올바른 지역을 선택했는지 확인합니다.

단계 1 EC2 Management Console로 이동합니다.

단계 2 **Launch Instance(**인스턴스 시작**)**를 클릭하고 드롭다운 목록에서 **Launch Instance(**인스턴스 시작**)**를 선택합니다.

단계 3 **AWS Marketplace**를 클릭합니다.

참고 Secure Email Gateway는 AWS Marketplace에서 사용할 수 없습니다. AMI 이미지를 프로비저닝하려면 AWS 계정 세부 정보(사용자 이름 및 지역)를 사용하여 Cisco 영업 담당자에게 문의하십시오.

단계 4 가상 어플라이언스 모델에 따라 인스턴스 유형을 선택합니다. 예를 들어 Secure Web 가상 어플라이언스 S300V 모델이 필요한 경우 c4.xlarge 및 해당 vCPU, vRAM 등을 선택합니다.

제품	**AsyncOS** 버전	모델	**EC2** 인스턴스 유형	**vCPU**	**vRAM**	**vNIC**	최소 디스크 크기
Cisco Secure Email Gateway 가상 어플라이언스	AsyncOS 14.0 이상(이메일)	**C100V**	c4.xlarge	4	7.5GB	1 (*)	200GB
		C300V	c4.2xlarge	8	15 GB	1 (*)	500GB
		C600V	c4.4xlarge	16	30GB	1 (*)	500GB

(*) 기본적으로 단일 NIC가 제공되지만 사용자가 인스턴스를 시작할 때 추가 인터페이스를 생성할 수 있습니다.

제품	**AsyncOS** 버전	모델	**EC2** 인스턴스 유형	**vCPU**	**vRAM**	**vNIC**	최소 디스크 크기
Cisco Secure Web Virtual Appliance	AsyncOS 14.5 이상(웹)	**S100V**	c5.xlarge	4	8GB	2	200GB
		S300V	c5.2xlarge	8	16GB	3	500GB
		S600V	c5.4xlarge	16	32GB	3	750GB
	AsyncOS 14.0 이상(웹)	**S100V**	m4.large	2	8GB	2	200GB
		S300V	c4.xlarge	4	7.5GB	3	500GB
		S600V	c4.4xlarge	16	30GB	3	750GB

제품	AsyncOS 버전	모델	EC2 인스턴스 유형	vCPU	vRAM	최소 디스크 크기
Cisco Secure Email 및 Web Manager 가상 어플라이언스	AsyncOS 14.0 이상	M100V	현재 이미지를 사용할 수 없습니다.	-	-	-
		M300V	c4.xlarge	4	7.5GB	1024GB
		M600V	c4.2xlarge	8	15 GB	2032GB

참고
- 7.5GB vRAM을 사용하여 C100V 및 S300V 어플라이언스를 구성하는 경우, 가상 머신 이미지가 잘못 구성되었거나 RAID 상태가 최적이 아니라는 경고 메시지가 표시됩니다. 이러한 경고 메시지는 **loadlicense** 및 **upgrade**와 같은 CLI 명령을 사용할 때 표시됩니다. 이 메시지는 무시하셔도 됩니다. vRAM 구성은 어플라이언스의 정상적인 작동에 영향을 주지 않습니다.
- Secure Web 가상 어플라이언스에서 분할 라우팅을 사용하는 경우 프록시 수신 포트에 공용 IP 주소(탄력적 IP)를 할당해야 합니다.

단계 **5** **Next: Configure Instance Details(**다음**:** 인스턴스 세부 정보 구성**)**를 클릭합니다.

Coeus 14.5 용 AWS에서 SWA(Secure Web Appliance) 구축

Coeus 14.5에 대한 AWS 스캔을 성공적으로 수행하려면 다음 단계를 수행합니다.

단계 **1** 다음 표에 나열된 각 **C4** 인스턴스 유형으로 AMI를 구축합니다.

모델	인스턴스 유형
S100V	m4.large
S300V	c4.2xlarge
S600V	c4.4xlarge

단계 **2** 인스턴스가 활성화되면 **SSH** 및 관리자 자격 증명을 사용하여 연결하여 연결성을 확인합니다.

단계 **3** Secure Web Appliance CLI를 사용하여 인스턴스를 종료하고 AWS CLI를 사용하여 인스턴스를 확인합니다.

단계 **4** 인스턴스를 업데이트하려면 AWS CLI를 액세스 키 ID 및 비밀 액세스 키와 연결합니다.

단계 **5** ENA가 EC2 인스턴스에서 이미 활성화되어 있는지 확인하려면 인스턴스 ID 및 지역을 사용하여 다음 명령을 실행합니다.

```
aws ec2 describe-instances --instance-id <your-instance-id> --query"Reservations[].Instances[].EnaSupport"
--region <your-region>
```

- ENA가 성공적으로 활성화되면 상태가 '**True**'로 반환됩니다. 단계 7를 진행합니다.

- ENA가 활성화되지 않은 경우 빈 문자열을 반환합니다. 다음 단계로 진행합니다.

단계 **6** EC2 인스턴스에서 ENA를 활성화하려면 다음 명령을 실행합니다.

```
aws ec2 modify-instance-attribute --instance-id <your-instance-id> --ena-support --region <your-region>
```

참고 이 명령은 출력을 반환하지 않습니다. 단계 5로 이동합니다.

단계 **7** 다음 표에 나열된 대로 인스턴스 유형을 **C4**에서 **C5**로 변경합니다.

모델	인스턴스 유형
S100V	c5.xlarge
S300V	c5.2xlarge
S600V	c5.4xlarge

단계 **8** 인스턴스를 시작합니다.

다음에 수행할 작업

참고 Coeus 14.0에서 coeus 14.5로의 AWS 인스턴스 업그레이드는 지원되지 않습니다. Coeus 14.5에서 새 인스턴스를 구축하는 것이 좋습니다.

coeus-14-0에서 실행 중인 AWS 인스턴스가 있고 새로 구축된 coeus 14.5 인스턴스를 로드하기 위한 호환 가능한 구성을 생성하려는 경우, coeus-14-0 instance를 coeus 14.5로 업그레이드합니다. 그런 다음 구성을 다운로드할 수 있습니다. 자세한 내용은 Cisco Secure Web Appliance 사용 설명서의 어플라이언스 구성 저장, 로드 및 재설정 항목을 참조하십시오(호환되는 Coeus 14.5 구성을 얻는 경우에만 권장됨).

새로 구축된 Coeus 14.5 인스턴스에서 호환되는 구성을 로드하는 절차는 Cisco Secure Web Appliance 사용 설명서의 어플라이언스 구성 파일 로드 항목을 참조하십시오.

자세한 내용:

- AWS CLI 설치 및 설정에 대해서는 다음을 참조하십시오.

  https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html.

- AWS CLI 사용을 위한 설정 및 사전 요구 사항 구성은 다음을 참조하십시오.

  https://docs.aws.amazon.com/cli/latest/userguide/getting-started-prereqs.html.

인스턴스 세부 정보 구성

단계 **1** 인스턴스 번호를 입력합니다.

참고 스팟 인스턴스 구매 옵션을 사용하면 AWS 클라우드에서 예비 컴퓨팅 용량을 구매할 수 있습니다. 자세한 내용은 Amazon EC2 설명서를 참조하십시오.

단계 **2** **Network(**네트워크**)** 드롭다운 목록에서 올바른 VPC를 선택합니다.

단계 **3** **Subnet(**서브넷**)** 드롭다운 목록에서 이 구축에 필요한 서브넷을 선택합니다.

단계 **4** **Auto-assign Public IP(**공용 **IP** 자동 할당**)** 드롭다운 목록에서 필요한 옵션을 선택합니다.

— **Use subnet setting (Enable)(**서브넷 설정 사용**(**활성화**))**을 선택하여 서브넷 설정에 지정된 설정에 따라 공용 IP 주소를 할당합니다.

— **Enable(**활성화**)**을 선택하여 이 인스턴스에 대한 공용 IP 주소를 요청합니다. 이 옵션은 공용 IP 주소에 대한 서브넷 설정을 재정의합니다.

— 자동 할당된 공용 IP가 필요하지 않은 경우 **Disable(**비활성화**)**을 선택합니다. 이 옵션은 공용 IP 주소에 대한 서브넷 설정을 재정의합니다.

단계 **5** IAM 역할을 선택합니다.

단계 **6** **Shutdown behavior(**종료 동작**)**를 선택합니다. **Stop(**중지**)**을 선택하는 것이 좋습니다.

주의 **Terminate(**종료**)**를 선택하면 인스턴스와 모든 데이터가 삭제됩니다.

단계 **7** (선택 사항) **Protect against accidental termination(**우연한 종료로부터 보호**)** 확인란을 선택합니다.

단계 **8** (선택 사항) 요구 사항에 따라 **Monitoring(**모니터링**)**, **EBS** 최적화 인스턴스, **Tenancy(**테넌시**)** 등의 다른 옵션을 검토하고 선택합니다.

단계 **9** **Network Interfaces(**네트워크 인터페이스**)**를 선택합니다.

- 필요한 경우 이전에 생성한 네트워크 인터페이스에서 인터페이스를 추가할 수 있습니다.
- 다른 네트워크 인터페이스를 추가하려면 **Add Device(**디바이스 추가**)**를 선택합니다. 인스턴스를 시작할 때 최대 2개의 네트워크 인터페이스를 지정할 수 있습니다. 인스턴스를 시작한 후 탐색창에서 **Network Interfaces(**네트워크 인터페이스**)**를 선택하여 추가 네트워크 인터페이스를 추가합니다.
- 둘 이상의 네트워크 인터페이스를 지정하는 경우 공용 IP 주소를 자동 할당할 수 없습니다.
- 인스턴스 유형에 대해 생성할 수 있는 네트워크 인터페이스의 최대 개수가 있습니다. 가상 어플라이언스 AMI 선택 및 인스턴스 유형 선택의 4단계를 참조하십시오.
- 고정 IP 주소를 생성하려면 탄력적 IP 주소 생성을 참조하십시오.

스토리지 구성 및 태그 추가

단계 **1** 기본 스토리지 옵션을 유지합니다. 필요에 따라 수정할 수 있습니다.

참고 모든 구축에 프로비저닝된 IOPS SSD를 사용하는 것이 좋습니다. 범용 SSD를 사용할 수 있지만 프로비저닝된 IOPS SSD가 최적의 성능을 제공합니다. 인스턴스가 처음으로 로그인할 수 있을 때까지 최대 45분이 걸릴 수 있습니다.

단계 **2** 필요한 태그를 입력합니다. 인스턴스에 대해 하나 이상의 태그를 생성할 수 있습니다.

예를 들어 *name*을 키로, 해당 값을 *Cisco wsa*로 지정합니다.

보안 그룹 구성, 인스턴스 검토 및 시작

단계 **1** 구축에 대한 올바른 보안 그룹을 선택합니다.

단계 **2** **Review and Launch(**검토 및 실행**)**를 클릭합니다.

단계 **3** 구성을 검토하고 모든 세부 사항이 요구 사항과 일치하는지 확인합니다.

단계 **4** 인스턴스를 시작합니다.

단계 **5** 기존 키 쌍을 선택하거나 새 키 쌍을 생성하고 다운로드합니다. 키 쌍 없이 인스턴스를 생성하는 것은 지원되지 않습니다.

단계 **6** **Launch(**실행**)**를 클릭하여 인스턴스를 실행합니다.

단계 **7** **Instances(**인스턴스**)**를 클릭합니다.

EC2 **Instances(**인스턴스**)** 페이지에서 새로 구성된 인스턴스를 볼 수 있습니다. 인스턴스의 확인에 성공하면 **Status Checks(**상태 확인**)** 열 아래에 녹색 확인 표시가 표시되고 그 뒤에 **2/2**개의 확인이 통과됨이 표시됩니다.

단계 **8** (선택 사항) 다음 단계를 수행하여 시스템 로그를 확인합니다.

1. **Instances(**인스턴스**)** 페이지에서 인스턴스를 선택합니다.
2. **Actions(**작업**)**를 클릭합니다.
3. **Instance Settings(**인스턴스 설정**)** 아래에서 **Get System Log(**시스템 로그 가져오기**)**를 클릭합니다.
4. 로그인 프롬프트가 표시되면 인스턴스가 작동 및 실행 중임을 나타냅니다.

단계 **9** (선택 사항) 인스턴스에 공용 IP를 할당하도록 선택한 경우 공용 IP 주소를 사용하여 액세스하는지 확인합니다.

시작된 인스턴스 구성

참고 Secure Web Appliance에서 기본 'admin' 사용자에 대한 SSH 액세스는 키 기반 인증만 사용합니다. 비밀번호 기반 인증은 **userconfig** CLI 명령 및 시스템 관리 > 사용자 아래의 애플리케이션 GUI를 사용하여 구성한 사용자에게 제공됩니다.

단계 **1** EC2 탐색 패널에서 **Instances(**인스턴스**)**를 클릭합니다.

단계 **2** 인스턴스를 선택하고 **Connect(**연결**)**를 클릭합니다.

단계 **3** **Connect to Your Instance(**인스턴스에 연결**)** 대화 상자에서 연결 정보를 검토합니다. SSH를 통해 가상 어플라이언스에 연결하려면 이 정보가 필요합니다. 여기에는 공용 DNS와 함께 사용되는 PEM 파일이 포함됩니다. 키가 공개적으로 표시되지 않도록 합니다.

참고 기본 사용자 이름은 `admin`이며 표시된 대로 root가 아닙니다.

단계 **4** SSH 클라이언트를 사용하여 인스턴스에 연결합니다.

단계 **5** CLI를 통해 라이선스를 붙여넣거나 파일에서 로드하려면 **loadlicense** 명령을 사용합니다.

참고 권장되는 7.5GB vRAM이 있는 C100V 및 S300V 어플라이언스의 경우 잘못 구성된 가상 머신 이미지 또는 RAID 상태가 최적이 아니라는 경고 메시지가 표시됩니다. 이러한 경고 메시지는 **loadlicense** 및 **upgrade**와 같은 CLI 명령을 사용할 때 표시됩니다. 이 메시지는 무시하셔도 됩니다. vRAM 구성은 어플라이언스의 정상적인 작동에 영향을 주지 않습니다.

단계 **6** 웹 인터페이스가 어플라이언스별 호스트 이름으로 응답하지 않도록 합니다. **adminaccessconfig > hostheader** CLI를 사용하고 변경 사항을 커밋합니다.

Cisco Secure Web Appliance 사용 설명서의 시스템 관리 작업 수행 장에서 어플라이언스 액세스를 위한 추가 보안 설정 항목을 참조하십시오.

어플라이언스의 웹 인터페이스에 연결

웹 인터페이스를 사용하여 어플라이언스 소프트웨어를 구성합니다. 인스턴스를 선택하면 IP 주소가 **Description(**설명**)** 탭에 표시됩니다. 기본 사용자 이름 및 비밀번호는 **admin** 및 **ironport**입니다.

다음 표에는 가상 어플라이언스의 기본 포트가 나와 있습니다.

제품	**HTTP** 포트	**HTTPS** 포트
Cisco Secure Web Appliance	8080	8443
Cisco Secure Email Gateway	80	443

제품	HTTP 포트	HTTPS 포트
Cisco Secure Email 및 Web Manager	80	443

예를 들어, 다음이 가능합니다.

- System Setup Wizard(시스템 설정 마법사) 실행

참고 IP 주소 및 기본 게이트웨이는 AWS에서 선택됩니다. 이러한 항목은 보존할 수 있습니다. 모든 악성코드를 Block(차단)으로 설정하는 것이 좋습니다.

- 컨피그레이션 파일을 업로드합니다.
- 수동으로 기능을 구성합니다.
- 필요한 정보 수집을 포함하여 어플라이언스를 액세스하고 구성하는 방법은 추가 정보의 관련 위치에서 제공되는 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.
- 물리적 어플라이언스에서 설정을 마이그레이션하려면 AsyncOS 릴리스에 대한 릴리스 정보를 참조하십시오.

해당 기능을 사용하도록 설정하기 전까지는 기능 키가 활성화되지 않습니다.

탄력적 IP 주소 생성

탄력적 IP 주소를 생성하려면 다음 단계를 수행하십시오.

단계 1 EC2 탐색창에서 **Elastic IPs(탄력적 IP)**를 클릭합니다.

단계 2 **Allocate new address(새 주소 할당)**를 클릭합니다.

단계 3 **Allocate(할당)**을 클릭합니다. 새 공용 IP 주소가 할당됩니다. IP 주소를 클릭하거나 **Close(닫기)**를 클릭할 수 있습니다.

단계 4 생성한 IP 주소를 선택합니다.

단계 5 **Actions(작업)**를 클릭하고 **Associate Address(주소 연결)**를 선택합니다.

단계 6 **Resource type(리소스 유형)**을 선택합니다.

단계 7 드롭다운 목록에서 인스턴스를 선택합니다.

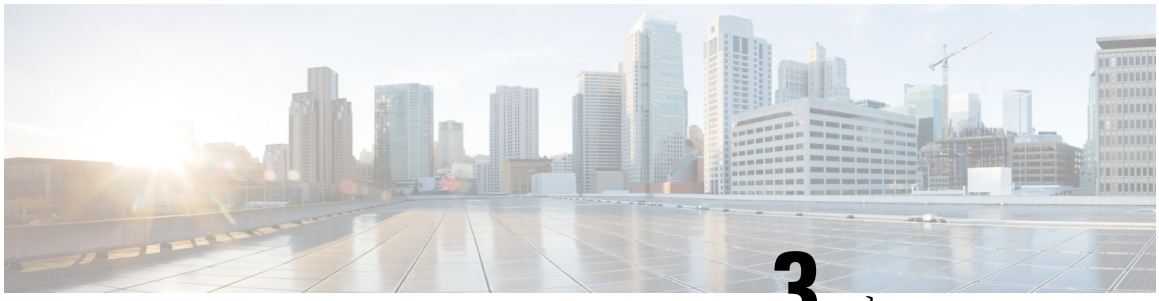
단계 8 탄력적 IP 주소를 연결할 프라이빗 IP 주소를 선택합니다.

단계 9 **Associate(연결)**를 클릭합니다.

단계 10 **Close(닫기)**를 클릭합니다.

라이선스 만료가 임박했을 때 알림을 보내도록 어플라이언스 구성

추가 정보의 관련 위치에서 제공되는 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.



3 장

가상 어플라이언스 관리

가상 어플라이언스 라이센스

참고 가상 어플라이언스 라이센스를 설치하기 전에는 기술 지원 터널을 열 수 없습니다. 기술 지원 터널에 대한 자세한 내용은 AsyncOS 릴리스의 사용 설명서를 참조하십시오.

Cisco Content Security Virtual Appliance에서는 호스트에서 가상 어플라이언스를 실행하려면 추가 라이센스가 필요합니다. 이 라이센스는 여러 개의 복제된 가상 어플라이언스에 사용할 수 있습니다.

Cisco Secure Email Gateway 및 Cisco Secure Web 가상 어플라이언스의 경우:

- 개별 기능에 대한 기능 키의 만료 날짜는 다를 수 있습니다.
- 가상 어플라이언스 라이센스가 만료된 후 어플라이언스는 SMTP 프록시(Cisco Secure Email Gateway), 웹 프록시(Cisco Secure Web Appliance)로서의 역할을 계속 수행하고, 180일 동안 보안 서비스 없이 격리된 메시지를 자동으로 처리합니다(Secure Email and Web Manager). 이 기간 중에는 보안 서비스가 업데이트되지 않습니다. Content Security Management 어플라이언스에서 관리자 및 최종 사용자는 격리를 관리할 수 없으나, 관리 어플라이언스는 관리되는 Secure Email Gateway 어플라이언스에서 격리된 메시지를 계속 승인하며 격리된 메시지의 예약 삭제가 이루어집니다.

참고 AsyncOS 버전 되돌리기의 영향에 대한 자세한 내용은 AsyncOS 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.

가상 어플라이언스 전원 끄기

강제 재설정, 전원 끄기, 재설정 옵션이 완전히 지원되지 않습니다. Secure Email Gateway, Secure Web 또는 Secure Email and Web Manager 가상 어플라이언스를 실행 중인 인스턴스를 종료하거나 중지할 수 있습니다.

가상 어플라이언스의 **CLI** 명령

다음은 가상 어플라이언스에 대한 CLI 명령 변경 사항입니다.

명령	가상 **Secure Email Gateway**에서 지원됨	가상 **Secure Web Appliance**에서 지원되는지 여부	가상 보안 **Secure Email and Web Manager**에서 지원되는지 여부	정보
loadlicense	예	예	예	가상 어플라이언스에 대한 라이센스를 설치할 수 있는 명령입니다. 이 명령을 먼저 사용하여 라이센스를 설치하지 않으면 가상 어플라이언스에서 시스템 설정 마법사를 실행할 수 없습니다.
etherconfig	예	예	—	가상 어플라이언스에는 페어링 옵션이 포함되지 않습니다.
version	예	예	—	이 명령은 UDI, RAID 및 BMC 정보를 제외하고 가상 어플라이언스에 대한 모든 정보를 반환합니다.
resetconfig	예	예	—	이 명령을 실행하면 가상 어플라이언스 라이센스 및 기능 키가 어플라이언스에 남겨집니다.
revert	예	예	—	동작은 어플라이언스에 대한 온라인 도움말 및 사용 설명서의 시스템 관리 장에 설명되어 있습니다.
reload	예	예	—	이 명령을 실행하면 가상 어플라이언스 라이센스 및 기능 키가 어플라이언스에서 제거됩니다. 이 명령은 Secure Web Appliance에만 사용할 수 있습니다.

명령	가상 **Secure Email Gateway**에서 지원됨	가상 **Secure Web Appliance**에서 지원되는지 여부	가상 보안 **Secure Email and Web Manager**에서지원되는지 여부	정보
diagnostic	예	예	—	다음의 **diagnostic > raid** 하위 메뉴 옵션은 정보를 반환하지 않습니다. **1.** 디스크 확인 실행 **2.** 진행 중인 작업 모니터링 **3.** 디스크 확인 결과 표시 이 명령은 Secure Web Appliance에만 사용할 수 있습니다.
showlicense	예	예	예	라이센스 세부 정보를 봅니다. 가상 Cisco Secure Web Appliance의 경우, **featurekey** 명령을 통해 추가 정보가 제공됩니다.

가상 어플라이언스의 **SNMP**

가상 어플라이언스의 AsyncOS는 하드웨어 관련 정보를 보고하지 않으며 하드웨어 관련 트랩도 생성되지 않습니다. 다음 정보가 쿼리에서 생략됩니다.

- `powerSupplyTable`
- `temperatureTable`
- `fanTable`
- `raidEvents`
- `raidTable`

가상 어플라이언스에 대한 지원 받기

참고 가상 어플라이언스에 대한 지원을 받으려면 Cisco TAC에 문의하거나 VLN(Virtual License Number) 번호를 준비하십시오.

Cisco Content Security 가상 어플라이언스에 대한 지원 사례를 생성하는 경우 계약 번호 및 PID(Product Identifier) 코드를 제공해야 합니다.

가상 어플라이언스에서 실행되는 소프트웨어 라이센스를 기반으로 PID를 식별할 수 있습니다. 구매 발주서를 참조하거나 다음 목록에서 확인할 수 있습니다.

- Cisco Secure Email Gateway 가상 어플라이언스의 PID(Product Identifier Code)
- Cisco Secure Web 가상 어플라이언스의 PID(Product Identifier Code)

Cisco Secure Email Gateway 가상 어플라이언스의 **PID(Product Identifier Code)**

기능	**PID**	설명
Cisco Secure Email	CSEMAIL-SEC-SUB	온프레미스, 클라우드 또는 하이브리드로 구축할 수 있는 Cisco Secure Email 소프트웨어 구독 라이선스입니다. 이 SKU(Stock Keeping Unit)는 선불 및 연간 청구 옵션만 허용합니다.
Essential		구성: • 안티스팸 필터링 • 아웃브레이크 필터링 • Sophos 안티 바이러스 필터링 • Cisco Secure Email Malware Defense - 평판 및 Cisco Threat Grid 샌드박싱 기능 포함
Advantage		구성: • 모든 필수 기능 • Cisco Secure Email 암호화 서비스 • Cisco Data Loss Protection(DLP)
Premier		구성: • 모든 Advantage 기능 • Cisco Secure Awareness 교육

기능	**PID**	설명
애드온 - 인텔리전스 멀티 스캔		여러 안티스팸 분류자의 결과를 인바운드 및 프리미엄 번들의 Cisco IPAS 분류자와 결합하여 추가 안티스팸 분류 기능을 제공합니다. 이로 인해 오탐이 더 많아질 수 있지만 스팸 탐지율이 높아집니다.
애드온: Graymail(그레이메일) 안전한 수신 거부		합법적인 마케팅 이메일을 수신한 사용자가 서드파티를 통해 안전하게 수신 거부할 수 있습니다.
애드온: McAfee Anti-Malware		인바운드 및 프리미엄 번들과 함께 제공되는 Sophos 안티바이러스 엔진에 대한 추가 안티바이러스 보호 기능을 제공합니다.
애드온: 이미지 분석기		허용되는 사용자 정책을 구현하기 위해 종종 DLP와 함께 구축되는 이메일에 포함된 이미지에서 성인 콘텐츠에 대한 검사를 제공합니다.
중앙 집중식 이메일 관리	SMA-EMGT-LIC	모든 중앙 집중식 보안 이메일 기능.

Cisco Secure Web 가상 어플라이언스의 **PID(Product Identifier Code)**

기능	**PID**	설명
Cisco Secure Web	WEB-SEC-SUB	Cisco Web Security 통합 SKU
Web Security Essentials	WSA-WSE-LIC	구성: • 웹 사용 제어 • 웹 평판
웹 보안 이점	WSA-WSP-LIC	구성: • 필수 기능 • Sophos 및 Webroot 안티멀웨어 시그니처

기능	**PID**	설명
웹 보안 프리미어	WSA-WSS-LIC	구성: • Advantage 기능 • Cisco Advanced Malware Protection • Cisco Cognitive Threat Analytics • Cisco Threat Grid
McAfee Anti-Malware	WSA-AMM-LIC	—
AMP(Advanced Malware Protection)	WSA-AMP-LIC	—
SMA 중앙 웹 관리	SMA-WMGT-LIC	모든 중앙 집중식 보안 웹 기능.
SMA 애드온: 고급 보고 - 상위 데이터 계층	SMA-WSPL-HIGH-LIC	—
SMA 애드온: 고급 보고 - 하위 데이터 계층	SMA-WSPL-LOW-LIC	—

Cisco TAC

Cisco TAC의 연락처 정보(전화번호 포함):

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

A 부록

추가 정보

추가 정보

지원 옵션에 대한 정보를 포함한 자세한 내용은 사용 중인 AsyncOS 릴리스의 릴리스 정보와 사용 설명서 또는 온라인 도움말을 참조하십시오.

Cisco Content Security 제품용 설명서:	위치:
Secure Email and Web Manager	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Secure Web Appliance	https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html
Secure Email Gateway	https://www.cisco.com/c/en/us/support/security/email-security-virtual-appliance/series.html

추가 정보