빠른 시작 설명서

Cisco M380 및 Cisco M680 Content Security Management Appliance

1 안녕하세요!
2 시작하기 전에
3 네트워크 설정 문서화
4 설치 계획
5 랙에 어플라이언스 설치
6 어플라이언스 연결
7 IP 주소 일시적 변경
8 어플라이언스에 연결
9 어플라이언스 전원 켜기
10 어플라이언스에 로그인
11 시스템 설정 마법사 실행
12 네트워크 설정 구성
13 컨피그레이션 요약
14 완료!
15 자주 묻는 질문(FAQ)
16 참고 자료

부품 번호: 78-21149-01

1 안녕하세요!

Cisco M380 및 Cisco M680 Content Security Management Appliance(Cisco M380 및 Cisco M680)를 선택해 주셔서 감사합니다.

Content Security Management Appliance는 중요한 정책 및 런타임 데이터를 중앙 집중화하고 통합하여 관리자와 엔드 유저에게 이메일 및 웹 보안 시스템을 관리할 수 있는 단일 인터페이스를 제공합니다. 또한 Cisco C-Series 및 S-Series 어플라이언스에서 최고의 성능을 보장하는 한편 구축 유연성을 높여 기업 네트워크 무결성을 보호합니다.

Content Security Management 어플라이언스는 Cisco Email & Web Security Appliance의 모든 보고 및 감사 정보를 관리하는 중앙 플랫폼을 제공합니다. 옵션 관리 기능을 사용하면 모든 보안 작업을 Content Security Management 어플라이언스 하나만 사용하여 조율하거나 로드를 여러 개의 어플라이언스로 분산할 수 있습니다.

본 설명서에서는 Cisco M380 및 Cisco M680 어플라이언스를 물리적으로 설치하는 방법과 System Setup Wizard(시스템 설정 마법사)를 사용하여 기본 설정을 구성하는 방법에 대해 설명합니다.

2 시작하기 전에

설치를 시작하기 전에 필요한 항목이 있는지 확인하시기 바랍니다. 다음 목품은Cisco M380 및 Cisco M680 Content Security Management Appliance에 포함되어 있습니다.

- 퀵 스타트 가이드(본 설명서)
- 슬라이드 레일 키트
- 전원 케이블(2)
- 네트워크에 어플라이언스를 연결하기 위한 이더넷 케이블
- 컴퓨터를 콘솔 포트에 연결하기 위한 RJ-45 to DB-9 케이블
- Cisco Content Security 설명서 포인터 카드

참고 Cisco M680 어플라이언스의 잠금 페이스플레이트(Faceplate) 버전에 두 개의 잠금 키가 포함되어 있습니다. 키를 분실했을 때 키를 교체하려면 4자리 키 코드가 필요하므로 이 키를 안전하게 보관하시기 바랍니다.

다음 품목은 직접 준비해야 합니다.

- 랙 캐비닛 인클로저(어플라이언스를 랙에 설치할 경우)
- 10/100/1000 Base TX TCP/IP LAN
- 데스크톱 또는 노트북 컴퓨터
- 웹 브라우저(또는 SSH 및 터미널 소프트웨어)
- 4 페이지의 "네트워크 설정 문서화" 섹션에 대한 네트워크 및 관리자 정보

3 네트워크 설정 문서화

시작하기 전에 네트워크 및 관리자 설정에 대한 다음 정보를 기록해 두십시오. 시스템 설정 마법사를 실행할 때 이 정보가 필요합니다.

시스템 설정	
기본 시스템 호스트 이름:	
예약 보고서 배달 대상:	
표준 시간대 정보:	
NTP 서버:	
관리자 비밀번호:	
자동지원:	사용/사용 안 함
네트워크 통합	
기본 게이트웨이(라우터) IP 주소:	
DNS(인터넷 또는 직접 지정):	
인터페이스	
데이터 포트 1	
IP 주소:	
네트워크 마스크:	
정규화된 호스트 이름:	
데이터 포트 2	
IP 주소:	
네트워크 마스크:	
잠금 앞판	
4자리 코드(M680-LKFP 어플라이언스의 경우)	

4 설치 계획

Cisco M380 및 Cisco M680 Content Security Management Appliance는 기업 정책 설정 및 감사 정보를 모니터링하기 위한 외부 위치의 역할을 하도록 설계되었습니다. 이 어플라이언스는 하드웨어, 운영 체제(AsyncOS) 및 지원 서비스를 조합하여 중요한 정책 및 런타임 데이터를 중앙 집중화 및 통합합니다.

Cisco M380 및 Cisco M680은 내부 DMZ 내에 설치하도록 설계되었으며 외부 DMZ의 Cisco C-Series 및 S-Series 어플라이언스에서 격리된 스팸을 수신합니다. 내부 사용자는 Content Security Management Appliance에 액세스하여 자신의 격리에서 메시지를 보고 관리합니다.

다음과 같이 네트워크 컨피그레이션을 계획합니다.

5 랙에 어플라이언스 설치

제공된 슬라이드 레일을 사용하여 Cisco M380 및 Cisco M680 Content Security Management Appliance를 설치합니다. 랙에 어플라이언스를 설치하는 방법은 *Cisco 380 및 Cisco 680 Series 하드웨어 설치 가이드*를 참조하시기 바랍니다.

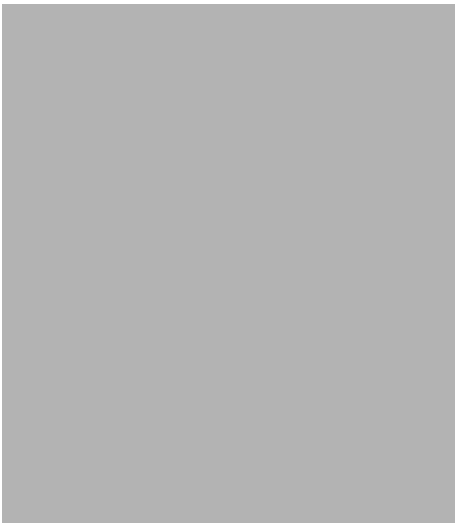
어플라이언스 배치

- 주변 온도 - 어플라이언스의 과열을 방지하기 위해 주변 온도가 104°F(40°C)를 넘는 곳에서 운영하지 마십시오.
- 공기 흐름 - 어플라이언스 주변에 적절한 공기 흐름이 있어야 합니다.
- 기계적 하중 - 위험한 상황을 방지하기 위해 어플라이언스는 수평을 이뤄야하며 안정적이어야 합니다.

6 어플라이언스 연결

각 직선 전원 케이블의 끝(암)을 어플라이언스 후면 패널에 있는 예비 전원 공급 장치에 연결합니다.

다른 쪽 끝(수)을 전기 콘센트에 연결합니다.



7 IP 주소 일시적 변경

Cisco M380 및 Cisco M680에 연결하려면 컴퓨터의 IP 주소를 일시적으로 변경해야 합니다.

참고 컨피그레이션을 완료한 후 이 설정으로 되돌려야 하므로 현재의 IP 컨피그레이션 설정을 메모해 두십시오.

Windows 용

1단계 Start(시작) 메뉴로 이동하여 **Control Panel(제어판)**을 선택합니다.

2단계 **Network and Sharing Center(네트워크 및 공유 센터)**를 더블클릭합니다.

3단계 **Local Area Connection(로컬 영역 연결)**을 클릭한 다음 **Properties(속성)**를 클릭합니다.

4단계 **Internet Protocol (TCP/IP)(인터넷 프로토콜(TCP/IP))**을 선택한 다음 **Properties(속성)**를 클릭합니다.

5단계 **Use the Following IP Address(다음 IP 주소 사용)**를 선택합니다.

6단계 다음과 같이 변경합니다.

- IP 주소: **192.168.42.43**
- 서브넷 마스크: **255.255.255.0**
- 기본 게이트웨이: **192.168.42.1**

7단계 **OK(확인)**와 **Close(닫기)**를 차례로 클릭하여 대화 상자를 닫습니다.

Mac

1단계 Apple 메뉴를 시작하고 **System Preferences(시스템 기본 설정)**를 선택합니다.

2단계 **Network(네트워크)**를 클릭합니다.

3단계 자물쇠 아이콘을 클릭하여 변경을 허용합니다.

4단계 녹색 아이콘이 있는 이더넷 네트워크 컨피그레이션을 선택합니다. 이 컨피그레이션이 활성 연결입니다. 다음으로 **Advanced(고급)**를 클릭합니다.

5단계 TCP/IP 탭을 클릭하고 이더넷 설정의 드롭다운 목록에서 **Manually(수동으로)**를 선택합니다.

6단계 다음과 같이 변경합니다.

- IP 주소: **192.168.42.43**
- 서브넷 마스크: **255.255.255.0**
- 라우터: **192.168.42.1**

7단계 **OK(확인)**를 클릭합니다.

8 어플라이언스에 연결

시스템 상자에 포함된 이더넷 케이블을 사용하여 관리 포트에 랩톱을 연결합니다. Cisco M380 및 Cisco M680 어플라이언스는 관리 포트만 사용합니다.

항목	포트	설명
1	콘솔	컴퓨터를 어플라이언스에 직접 연결하는 콘솔 포트를 나타냅니다.
2	관리 인터페이스	관리용으로만 제한되는 기가비트 이더넷 인터페이스를 나타냅니다. RJ-45 케이블을 사용하여 연결합니다.
3	데이터 1	기가비트 이더넷 고객 데이터 인터페이스 데이터 1을 나타냅니다.
4	데이터 2	기가비트 이더넷 고객 데이터 인터페이스 데이터 2를 나타냅니다.
5	데이터 3	기가비트 이더넷 고객 데이터 인터페이스 데이터 3을 나타냅니다.

참고 어플라이언스와 함께 NIC 카드를 주문한 경우 *Cisco 380 및 Cisco 680 Series 하드웨어 설치 설명서*의 PCI NIC 슬롯 컨피그레이션 섹션에서 자세한 내용을 참조하시기 바랍니다.

9 어플라이언스 전원 켜기

Cisco M380 및 Cisco M680의 전면 패널에 있는 On/Off 스위치를 눌러 어플라이언스 전원을 켭니다. 시스템 전원을 켤 때마다 시스템이 초기화될 때까지 5분을 기다려야 합니다. 시스템 전원이 켜진 후에는 어플라이언스가 작동 가능함을 나타내는 녹색등이 켜집니다.

참고 어플라이언스에 전원을 연결하고 곧바로 전원을 켜면 어플라이언스가 켜지고 팬이 회전하고 LED가 켜집니다. 그리고 30-60초 내에 팬이 멈추고 모든 LED가 꺼집니다. 31초 후에 어플라이언스 전원이 켜집니다. 이 동작은 시스템 펌웨어 및 컨트롤러를 동기화하기 위한 설계에 따른 것입니다.

10 어플라이언스에 로그인

웹 기반 인터페이스 또는 CLI(Command Line Interface)의 두 인터페이스 중 하나를 사용하여 Cisco M380 및 Cisco M680에 로그인할 수 있습니다.

웹 기반 인터페이스

1단계 이더넷 포트를 통해 웹 브라우저에 액세스하려면(9 페이지의 "어플라이언스에 연결" 섹션 참조) 웹 브라우저에서 다음 URL을 입력하여 Cisco M380 및 Cisco M680 어플라이언스 관리 인터페이스로 이동합니다.

http://192.168.42.42:8080

2단계 다음 로그인 정보를 입력합니다.

- 사용자 이름: **admin**
- 비밀번호: **ironport**

참고 호스트 이름 매개변수는 시스템 설정 과정에서 할당됩니다. 호스트 이름(http://hostname:8080)을 사용하여 관리 인터페이스에 연결하려면 어플라이언스 *호스트 이름*과 IP 주소를 DNS 서버 데이터베이스에 추가해야 합니다.

3단계 **Login(로그인)**을 클릭합니다.

CLI(Command Line Interface)

1단계	시리얼 포트를 통해 CLI(Command Line Interface)에 액세스하려면(9 페이지의 "어플라이언스에 연결" 섹션 참조) 9600비트, 8비트, 패리티 없음, 1 중지 비트(**9600, 8, N, 1**)를 사용하여 흐름 제어를 하드웨어로 설정하여 CLI(Command Line Interface) 터미널에 액세스합니다.
2단계	IP 주소 **192.168.42.42**로 텔넷 또는 SSH 세션을 시작합니다.
3단계	비밀번호 **ironport**를 사용하여 **admin**으로 로그인합니다.
4단계	프롬프트에서 **systemsetup** 명령을 실행합니다.

11 시스템 설정 마법사 실행

시스템 설정 마법사를 실행하여 기본 설정을 구성하고 시스템 기본값 세트를 활성화합니다. 시스템 설정 마법사는 웹 기반 인터페이스를 통해 어플라이언스에 액세스할 때(또는 CLI(Command Line Interface)에서 **systemsetup** 명령을 실행할 때) 자동으로 시작되며 엔드 유저 라이센스 계약(EULA)을 표시합니다.

1단계 시스템 설정 마법사를 시작합니다.

2단계 엔드 유저 라이센스 계약에 동의합니다.

3단계 등록 정보를 입력합니다.

4단계 4 페이지의 "네트워크 설정 문서화" 섹션의 정보를 입력합니다.

5단계 웹 보안 설정을 지정합니다.

6단계 컨피그레이션 요약 페이지를 검토합니다.

7단계 사용자 이름 **admin**과 시스템 설정 마법사에서 설정한 새 비밀번호를 사용하여 어플라이언스에 다시 로그인합니다.

Cisco M380 및 Cisco M680 Content Security Management Appliance는 자체 서명 인증서를 사용하므로 웹 브라우저에서 경고가 나타날 수 있습니다. 인증서를 승인하고 이 경고를 무시할 수 있습니다.

8단계 새 관리자 비밀번호를 기록하여 안전한 곳에 보관합니다.

12 네트워크 설정 구성

사용자의 네트워크 컨피그레이션에 따라 방화벽에서 다음 포트를 사용한 액세스를 허용하도록 구성해야 할 수도 있습니다. SMTP 및 DNS 서비스가 인터넷에 액세스할 수 있어야 합니다.

- DNS: 포트 53
- SMTP: 포트 6025 및 25

다른 시스템 기능의 경우, 다음 서비스가 필요할 수 있습니다.

- FTP: 포트 21, 데이터 포트 TCP 1024 이상
- HTTP: 포트 80 또는 82
- HTTPS: 포트 83 또는 443
- LDAP: 포트 389 또는 3268
- LDAP over SSL: 포트 636
- 글로벌 카탈로그 쿼리용 SSL을 통한 LDAP: 포트 3269
- NTP: 포트 123
- 격리 인증: 110(POP) 및/또는 143(IMAP)
- SSH: 포트 22
- 텔넷: 포트 23

참고 포트 443을 열지 않은 경우 기능 키를 다운로드할 수 없습니다.

자세한 내용은 *Cisco AsyncOS for Content Security Management 사용자 설명서*의 부록 "방화벽 정보"를 참조하시기 바랍니다.

경고 **대기열 및 컨피그레이션 파일의 손상을 방지하기 위해 System Administration(시스템 관리) > Shutdown/Reboot(종료/재부팅) 페이지에서 어플라이언스를 종료해야 합니다.**

13 컨피그레이션 요약

컨피그레이션의 다음 세부 사항을 검토합니다.

항목	설명
Management(관리)	시스템 설정 마법사를 완료했을 때 어플라이언스에 할당된 호스트 이름 또는 http://192.168.42.42를 입력하여 관리 포트(데이터 1)에서 콘텐츠 보안 관리 어플라이언스를 관리할 수 있습니다. 컨피그레이션을 공장 기본 설정으로 재설정한 경우에는(예를 들어 시스템 설정 마법사를 다시 실행하여) 데이터 1 포트(http://192.168.42.42)에서만 관리 인터페이스에 액세스할 수 있으므로 데이터 1 포트에 연결했는지 확인하시기 바랍니다. 또한 관리 인터페이스에서 HTTP에 대한 방화벽 포트 80 또는 82, HTTPS에 대한 포트 83 및 443을 열었는지 확인하시기 바랍니다.
Computer Address (컴퓨터 주소)	컴퓨터 IP 주소를 4 페이지의 "네트워크 설정 문서화" 섹션에서 메모했던 원래 설정으로 변경하는 것을 잊지 마십시오. **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)** 페이지에서 시스템 설정의 요약을 검토할 수 있습니다.

14 완료!

축하합니다. 이제Cisco M380 및 Cisco M680 Content Security Management Appliance를 사용할 준비가 되었습니다. 어플라이언스를 최대한 활용하기 위해 다음 조치 중 몇 가지를 수행하도록 고려할 수 있습니다.

보안 어플라이언스 추가

관리할 Cisco Email Security Appliance 및 Cisco Web Security Appliance를 추가할 수 있습니다. Cisco Security 어플라이언스를 Cisco M380 및 Cisco M680에 추가하려면 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)**를 선택합니다.

중앙 집중식 이메일 및 웹 보고 사용

Cisco M380 및 Cisco M680 Content Security Management Appliance는 이메일 보고 및 웹 보고 이외에도 여러 Email & Web Security Appliance의 이메일 및 웹 트래픽을 중앙 집중식으로 볼 수 있는 추적 기능도 지원합니다.

중앙 집중식 이메일 보고를 사용하도록 설정하려면 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Email(이메일) > Centralized Reporting(중앙 집중식 보고)**을 선택합니다.

중앙 집중식 웹 보고를 사용하도록 설정하려면 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Web(웹) > Centralized Reporting(중앙 집중식 보고)**을 선택합니다.

중앙 집중식 보고를 사용하도록 설정한 후에는 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Email(이메일) > Centralized Reporting(중앙 집중식 보고) 또는 Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Web(웹) > Centralized Reporting Overview(중앙 집중식 보고 개요)** 페이지에서 웹 및 이메일 보고에 대한 통계와 정보를 볼 수 있습니다.

메시지 추적

Message Tracking(메시지 추적) 서비스를 사용하여 쿼리를 실행하여(GUI에서) 메시지 배달 및 차단에 대한 세부 정보를 볼 수 있습니다.

이메일 보안 어플라이언스에 대한 메시지 추적에 액세스하려면 Monitor(모니터) > Message Tracking(메시지 추적)을 선택합니다.

이메일 및 웹 보고 예약

Cisco M380 및 Cisco M680 Content Security Management Appliance에서는 Email 또는 Web Security Appliance에서 수신되는 데이터를 이용하여 예약된 보고서를 생성할 수 있습니다. 보고서는 매일, 매주 또는 매월 실행하도록 예약할 수 있으며 전날, 이전 7일 또는 이전 달 데이터를 포함하도록 구성할 수 있습니다.

추가 정보

기타 Cisco M380 및 Cisco M680 어플라이언스에 구성할 수 있는 다른 기능이 있습니다. 사용 가능한 다른 기능에 대한 자세한 내용은 Content Security Management Appliance 설명서를 참조하시기 바랍니다.

15 자주 묻는 질문(FAQ)

Q. 내 Cisco M380 및 Cisco M680 Content Security Management Appliance에서 이전 컨피그레이션 마스터를 삭제하려면 어떻게 합니까?

A. **Web(웹) > Utilities(유틸리티) > Security Services Display(보안 서비스 표시)** 페이지로 이동하여 **Edit Settings(설정 편집)**를 클릭합니다. 각 컨피그레이션 마스터의 맨 위에서 해당하는 컨피그레이션 마스터 확인란을 선택 취소할 수 있습니다. **Submit (제출)**을 클릭하면 컨피그레이션 마스터가 더 이상 GUI의 Configuration(컨피그레이션) 탭에 표시되지 않습니다.

Q. 내 Cisco M380 및 Cisco M680 Content Security Management Appliance에 어플라이언스를 추가하려면 어떻게 합니까?

A. 일단 Cisco M380 및 Cisco M680 어플라이언스에서 모니터링 서비스를 사용하도록 설정하면, 관리하는 어플라이언스에 대한 연결 정보를 추가할 수 있습니다. AsyncOS 6.0 이상

을 사용하는 모든 Cisco Email Security Appliance 또는 AsyncOS 5.7, 6.3, 7.1 이상을 실행하는 모든 Cisco Web Security Appliance에 연결할 수 있습니다.

a. Cisco M380 및 Cisco M680 Content Security Management Appliance에서 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)**를 선택합니다.

b. **Add Email Appliance(이메일 어플라이언스 추가)**를 클릭하여 Add Email Security Appliance(이메일 보안 어플라이언스 추가) 페이지를 표시하거나 **Add Web Appliance(웹 어플라이언스 추가)**를 클릭하여 Add Web Security Appliance(웹 보안 어플라이언스 추가) 페이지를 표시합니다.

c. Appliance Name(어플라이언스 이름) 및 IP Address(IP 주소) 텍스트 필드에 Cisco 어플라이언스의 어플라이언스 이름과 관리 인터페이스 IP 주소를 입력합니다.

d. Cisco 어플라이언스를 관리할 때 사용할 서비스를 선택합니다.

e. **Establish Connection(연결 설정)**을 클릭합니다.

f. **Test Connection(연결 테스트)**을 클릭하여 원격 어플라이언스의 모니터링 서비스가 올바르게 구성되어 있으며 호환되는지 여부를 확인합니다.

g. Web Security Appliance를 추가할 때는 어플라이언스를 할당할 컨피그레이션 마스터를 선택합니다.

h. **Submit(제출)**을 클릭하여 페이지의 변경 사항을 제출한 다음 **Commit Changes(변경 사항 적용)**를 클릭하여 변경 사항을 적용합니다.

Q. 액세스 로그를 Web Security Appliance에서 Content Security Management Appliance로 전달해야 합니까?

A. 아니요. Centralized Reporting(중앙 집중식 보고)을 사용하도록 설정하면 이 기능이 Web Security Appliance에서 내부적으로 처리됩니다. Centralized Reporting(중앙 집중식 보고)을 사용하도록 설정하려면 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Web(웹) > Centralized Reporting(중앙 집중식 보고)**으로 이동하시기 바랍니다.

Q. Web Reporting 도구에서는 데이터가 얼마나 오래 보존됩니까?

A. 데이터 보존은 전체적인 사용량, 즉 레코드 수에 따라 달라집니다. 하지만 각 어플라이언스는 최소 45일의 보고를 수용할 수 있습니다.

Q. 내 웹 보고서에서 사용자 이름을 숨기려면 어떻게 합니까?

a. Cisco M380 및 Cisco M680 Content Security Management Appliance에서 **Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Web(웹) > Centralized Reporting(중앙 집중식 보고)**을 선택합니다.

b. **Edit Settings(설정 편집)**를 클릭합니다.

c. Reports(보고서) 확인란에서 Anonymize User Names(익명 사용자 이름)를 선택합니다.

d. **Submit(제출)**을 클릭합니다.

Q. 보고 데이터는 얼마나 자주 업데이트됩니까?

A. Cisco M380 및 Cisco M680 Content Security Management Appliance는 약 15분마다 관리되는 모든 어플라이언스에서 모든 보고서에 대한 데이터를 가져오고 이러한 어플라이언스의 데이터를 집계합니다. 어플라이언스에 따라 특정 메시지가 Content Security Management Appliance에서 보고 데이터에 포함될 때까지 시간이 걸릴 수 있습니다. 데이터에 대한 정보는 System Status(시스템 상태) 페이지에서 확인할 수 있습니다.

16 참고 자료

지원	
Cisco 지원 포털	http://www.cisco.com/support
미국 및 캐나다 수신자 부담 전화 번호	800-553-2447
국제 연락처	전 세계 전화 번호
이메일:	tac@cisco.com

Cisco Email Security 지원 커뮤니티 Cisco Web Security 지원 커뮤니티 (Content Security Management Appliance 지원 포함)	https://supportforums.cisco.com/community/netpro/security/email https://supportforums.cisco.com/community/netpro/security/web
제품 설명서	
Cisco M380 및 Cisco M680 Content Security Management Appliance 빠른 시작 설명서 (본 문서)	http://www.cisco.com/en/US/docs/security/security_management/sma/hw/quick_start/M380_M680_QSG_78_21149.pdf
Cisco 380 및 Cisco 680 Series 하드웨어 설치 설명서 LED, 기술 사양 및 장착 옵션에 대한 정보가 포함되어 있습니다.	http://www.cisco.com/en/US/docs/security/esa/hw/380_680_Series_HW_Install.pdf
Cisco Content Security Management Appliance 설명서 어플라이언스 기능 구성, CLI 명령 및 릴리스 정보에 설명서가 포함되어 있습니다.	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
안전 및 규정 준수 설명서	http://www.cisco.com/en/US/docs/security/content_security/compliance/ContentSecurity_regulatory_compliance_information.fm
MIB	
AsyncOS MIBs for Cisco Content Security Management Appliance(관련 도구 섹션)	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

설명서 받기 및 서비스 요청 제출

설명서 받기, 서비스 요청 제출 및 추가 정보 수집에 대한 자세한 내용은 http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html에서 *Cisco Product Documentation의 새로운 사항*을 참조하시기 바랍니다.

Cisco의 새로운 기술 문서 및 개정된 기술 문서를 모두 나열하는 *Cisco Product Documentation의 새로운 사항*을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 배달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco 및/또는 자회사의 상표 또는 등록 상표입니다. Cisco 상표의 목록을 보려면 www.cisco.com/go/trademarks로 이동하시기 바랍니다. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어의 사용이 Cisco와 다른 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소는 실제 주소가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력 및 그림은 이해를 돕기 위한 자료일 뿐입니다. 실제 IP 주소가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

© 2013년 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco 는 전 세계 200 곳 이상의 지사를 갖추고 있습니다 . 각 지사의 주소 , 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices** 에서 확인하시기 바랍니다 .

10% 재생 용지가 포함된 재활용 용지로 미국에서 인쇄

부품 번호 : 78-21149-01