게이트웨이, 클라우드 게이트웨이, Email and Web Manager의 파일 분석 클라이언트 ID 설명

목차

소개

이 문서에서는 Cisco Secure Email Gateway, Cloud Gateway, Email and Web Manager의 파일 분석 클라이언트 ID를 찾는 방법에 대해 설명합니다. File Analysis Client ID는 게이트웨이, 클라우드 게이트웨이 또는 Email and Web Manager가 파일 제출 및 샌드박싱을 위해 Cisco Malware Analytics(이전의 Threat Grid)에 등록할 때 사용되는 고유한 65자 등록 키입니다. 예를 들어, File Analysis 서비스를 활성화했지만 평판 서비스에 메시지에 첨부 파일에 대한 정보가 없고 첨부 파일이 분석할 수 있는 파일 기준을 충족하는 경우(File Reputation and Analysis Services의 지원 파일 참조), 메시지를 격리할 수 있습니다(분석을 위해 전송된 첨부 파일로 메시지 격리 참조), 분석을 위해 전송된 파일입니다.

"Appliance Grouping for File Analysis Reporting"의 경우 파일 분석 ID를 알고 있어야 합니다.

자세한 내용은 사용 설명서의 "파일 평판 필터링 및 파일 분석" 장을 참조하십시오.

- Cisco Secure Email Gateway 최종 사용자 설명서
- Cisco Secure Email Cloud Gateway 최종 사용자 설명서

게이트웨이, 클라우드 게이트웨이, 이메일 및 웹 관리자용 파일 분석 클라이언트 ID

File Analysis(파일 분석)를 활성화하면 어플라이언스에 대한 File Analysis Client ID가 자동으로 생성됩니다.

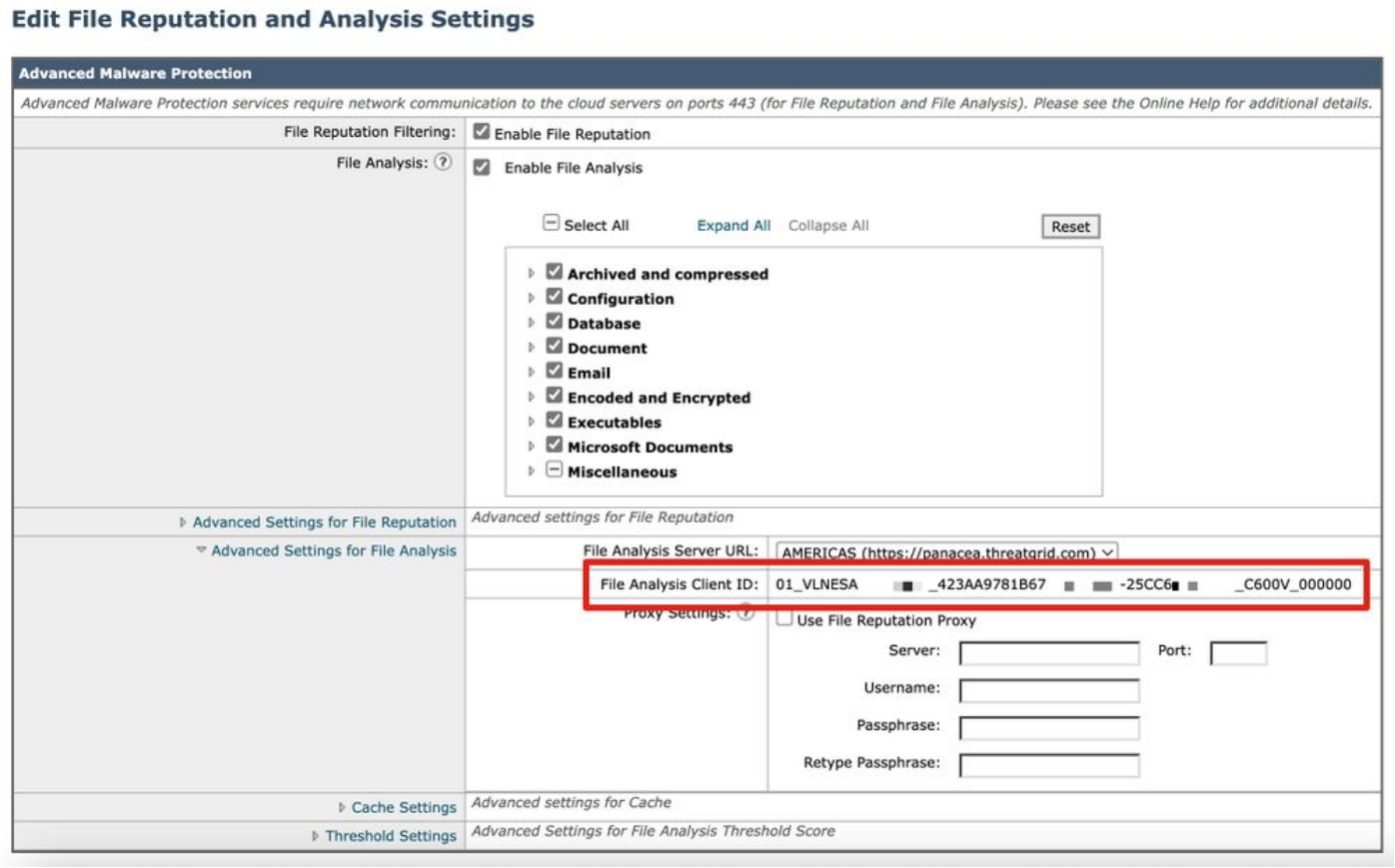
게이트웨이 또는 클라우드 게이트웨이에서 시작하기 전에 필요한 기능 키를 가지고 있고 파일 평판 및 파일 분석을 활성화했는지 확인하십시오. 기능 키를 보려면 **System Administration > Feature Keys로 이동합니다**. File Reputation(파일 평판)과 File Analysis(파일 분석)는 별도로 나열되며 Active(활성) 상태입니다.

게이트웨이 또는 클라우드 게이트웨이

1. 사용자 인터페이스에 로그인합니다.
2. **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)로 이동합니다.**
3. 전역 **설정 편집...을 클릭합니다.**
4. Advanced **Settings for File Analysis(파일 분석을 위한 고급 설정)를 확장합니다**.

파일 분석 클라이언트 ID가 여기에 나열됩니다.

E예:



참고: 가상 어플라이언스의 File Analysis Client ID는 하드웨어 어플라이언스와 다릅니다.

게이트웨이 또는 클라우드 게이트웨이의 파일 분석 클라이언트 ID는 65자 문자열 형식을 기반으로 합니다.

가치	설명

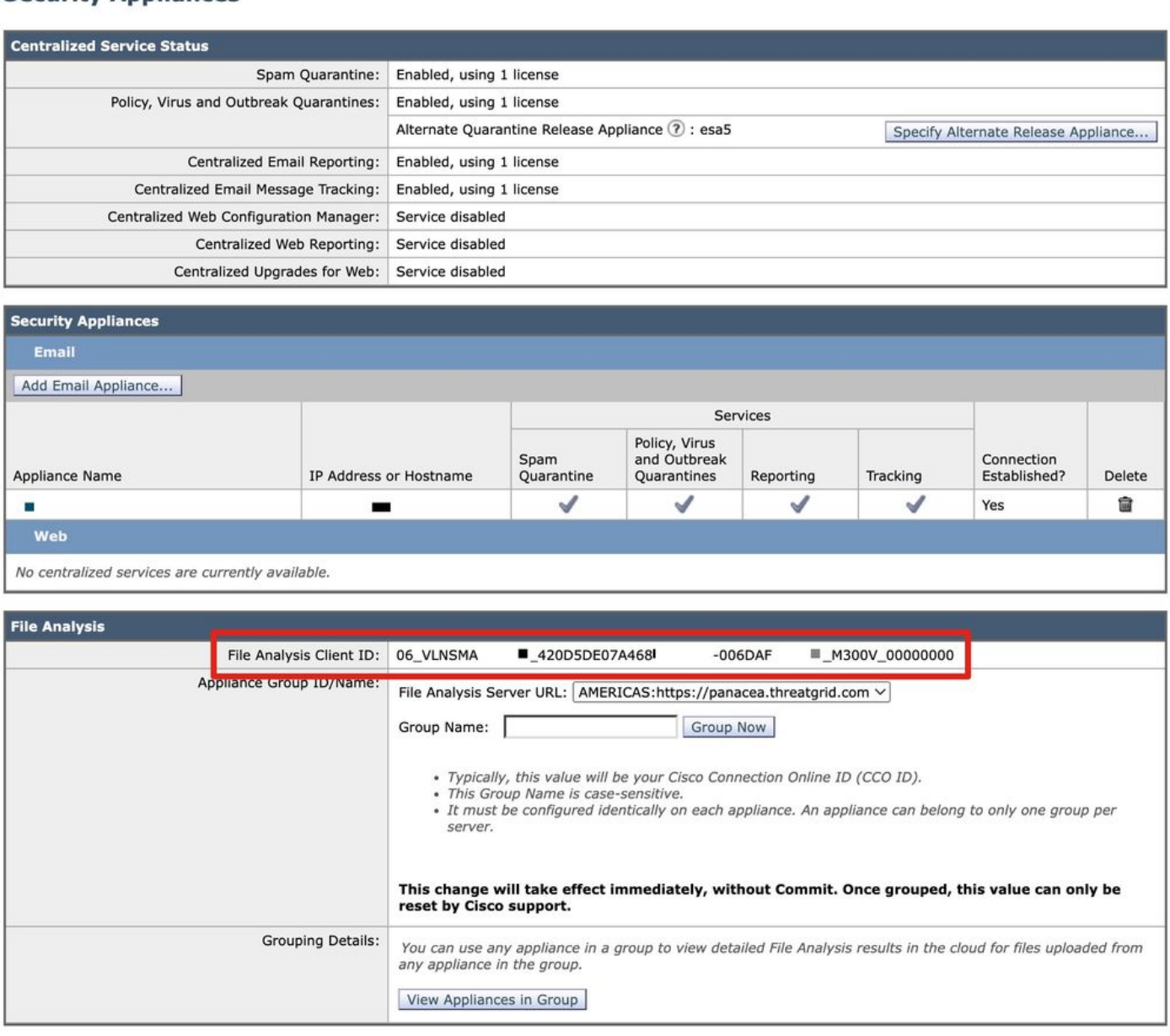
01_	"01"은 게이트웨이 또는 클라우드 게이트웨이에 한정됩니다.
VNESAXXXYYY_	가상 어플라이언스인 경우 VLAN 라이센스 번호(CLI 명령 showlicense에서 발견)를 **사용다**. 하드웨어 어플라이언스인 경우 필드가 없습니다.
직렬_	어플라이언스의 전체 시리얼
CX00V_	어플라이언스의 모델입니다.
00000000	필드 0. 이전 필드를 기준으로 이 필드는 65자의 필드를 완성하기 위해 다양합니다.

이메일 및 웹 관리자

1. 사용자 인터페이스에 로그인합니다.
2. Centralized Management(**중앙 집중식 관리) > Security Appliance(보안 어플라이언스)로 이동합니다**.

이 페이지의 하단에는 파일 분석 섹션이 있습니다. 파일 분석 클라이언트 ID가 여기에 나열됩니다.

예:



참고: 가상 어플라이언스의 File Analysis Client ID는 하드웨어 어플라이언스와 다릅니다.

Email 및 Web Manager의 파일 분석 클라이언트 ID는 65자 문자열 형식을 기반으로 합니다.

가치	설명
06_	"06"은 Email 및 Web Manager에만 해당됩니다.
VLNSMAXXYYY_	가상 어플라이언스인 경우 VLAN 라이센스 번호(CLI 명령 showlicense에서 발견)를 **사용다**. 하드웨어 어플라이언스인 경우 필드가 없습니다.
직렬_	어플라이언스의 전체 시리얼
MX00V_	어플라이언스의 모델입니다.
000000	필드 0. 이전 필드를 기준으로 이 필드는 65자의 필드를 완성하기 위해 다양합니다.

파일 분석 보고를 위한 어플라이언스 그룹화

라이센스에 Cisco Secure Malware Analytics(https://panacea.threatgrid.com)에 대한 액세스가 포함된 경우 게이트웨이 또는 클라우드 게이트웨이의 모범 사례는 개별 조직 계정과 연결되는 것입니다. 조직의 모든 콘텐츠 보안 어플라이언스가 조직의 게이트웨이 또는 클라우드 게이트웨이에서 분석을 위해 전송된 파일에 대한 자세한 결과를 클라우드에 표시하도록 하려면 모든 어플라이언스를 동일한 어플라이언스 그룹에 가입시켜야 합니다. Malware Analytics에 로그인하면 분석을 위해 클라우드로 전송된 제출 및 위협 샘플이 모두 조직의 Malware Analytics 대시보드에 표시됩니다.

참고: Cloud Gateway 고객은 Cisco에서 수행하는 활성화 및 구축 과정에서 이를 구성했습니다.

그룹 어플라이언스

참고: 클라우드 게이트웨이가 있는데 완료되지 않은 경우, 어플라이언스 그룹 ID/이름을 구성하기 전에 지원 케이스를 여십시오.

게이트웨이 또는 클라우드 게이트웨이

1. 사용자 인터페이스에서 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)로 이동합니다**.
2. **Click here(여기를 클릭하여 파일 분석 보고를 위한 어플라이언스를 그룹화하거나 봅니다**.
3. 어플라이언스 **그룹 ID/이름을 입력합니다**. 기본값은 다음과 같습니다. 이 값에는 CCOID를 사용하는 것이 좋습니다.어플라이언스는 하나의 그룹에만 속할 수 있습니다.파일 분석 기능을 구성한 후 그룹에 시스템을 추가할 수 있습니다.
4. **지금** 그룹**을 클릭합니다**.

이메일 및 웹 관리자

참고: 어플라이언스 그룹 ID/이름을 구성하는 옵션은 Email and Web Manager에 중앙 집중식 관리를 위해 추가된 Email Appliance가 있고 Policy, Virus, Outbreak Quarantines가 마이그레이션된 후에만 사용할 수 있습니다.

1. 사용자 인터페이스에서 Centralized **Services(중앙 서비스) > Security Appliances(보안 어플라이언스)로 이동합니다**. 어플라이언스 **그룹 ID/이름을 입력합니다**. 기본값은 다음과 같습니다 .일반적으로 이 값은 CCO ID(Cisco Connection Online ID)입니다.이 그룹 이름은 대/소문자를 구분합니다.각 어플라이언스에서 동일하게 구성해야 합니다. 어플라이언스는 서버당 하나의 그룹에만 속할 수 있습니다.
2. **지금** 그룹**을 클릭합니다**.

참고:

- 그룹 ID를 추가하면 커밋 없이 즉시 적용됩니다. 그룹 ID를 변경해야 하는 경우 Cisco TAC에 문의해야 합니다.
- 이 이름은 대/소문자를 구분하며 분석 그룹의 각 어플라이언스에서 동일하게 구성해야 합니다.

어플라이언스 보기

게이트웨이 또는 클라우드 게이트웨이

1. 사용자 인터페이스에서 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)로** 이동합니다**.**
2. **Click here(여기를 클릭하여 파일 분석 보고를 위한 어플라이언스를 그룹화하거나 봅니다**.
3. View Appliances(어플라이언스 **보기)를 클릭합니다**.

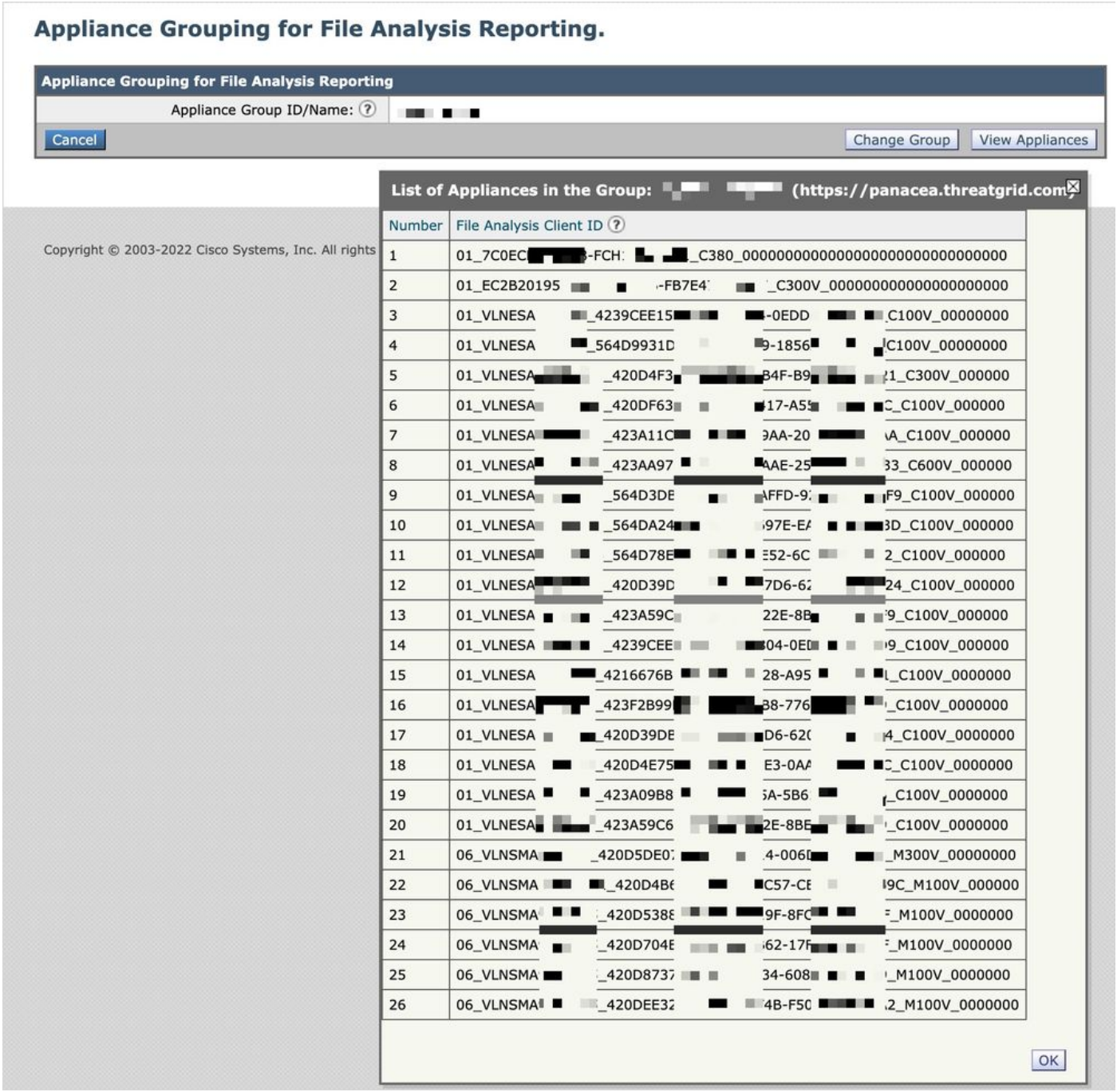
이메일 및 웹 관리자

1. 사용자 인터페이스에서 Centralized **Services(중앙 서비스) > Security Appliances(보안 어플라이언스)로 이동합니다**.
2. File Analysis(파일 분석) **섹션**에서 View Appliances in Group(그룹의 어플라이언스 보기)을 클

릭합니다.

어플라이언스 그룹 ID/이름과 연결된 모든 어플라이언스의 File Analysis Client ID(파일 분석 클라이언트 ID)가 여기에 나열됩니다.

예:



추가 정보

Cisco Secure Email Gateway 설명서

- 릴리스 정보

- 사용 설명서
- CLI 참조 가이드
- Cisco Secure Email Gateway용 API 프로그래밍 가이드
- Cisco Secure Email Gateway에서 사용되는 오픈 소스
- Cisco Content Security Virtual Appliance 설치 설명서(vESA 포함)

Secure Email Cloud Gateway 설명서

- 릴리스 정보
- 사용 설명서

Cisco Secure Email and Web Manager 설명서

- 릴리스 정보 및 호환성 매트릭스
- 사용 설명서
- Cisco Secure Email and Web Manager용 API 프로그래밍 가이드
- Cisco Content Security Virtual Appliance 설치 설명서(vSMA 포함)

Cisco Secure Malware Analytics

- Cisco Secure Malware Analytics(Threat Grid)

Cisco Secure Product 문서

- Cisco Secure 포트폴리오 명명 아키텍처

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.