



AsyncOS 12.0 for Cisco Email Security Appliances CLI 참조 가이드 - GD(일반 구축)

초판: 2019년 1월 31일

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

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패키지에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 퍼블릭 도메인 버전의 일부로서 University of Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급자의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급자는 상품성, 특정 목적에의 적합성, 타인의 권리 침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급업체는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급업체가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

모든 인쇄된 사본 및 이 문서의 중복된 소프트 복사본은 제어 대상이 아닌 것으로 간주됩니다. 최신 버전에 대한 현재 온라인 버전을 참조하십시오.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소 및 전화번호는 Cisco 웹사이트(www.cisco.com/go/office)에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks)로 이동하십시오. 언급된 타사 상표는 해당 소유권자의 재산입니다. '파트너'라는 용어의 사용이 Cisco와 다른 회사 간의 파트너십 관계를 의미하는 것은 아닙니다. (1721R)

© 2019 Cisco Systems, Inc. 모든 권리 보유.



목 차

서문:

서론	xxxiii
이 책을 읽기 전에	xxxiii
표기 규칙	xxxiii
추가 리소스	xxxiv

장 1

CLI 빠른 참조 설명서	1
CLI 명령(커밋 불필요)	1
CLI 명령(커밋 필요)	7

장 2

명령행 인터페이스: 기초	13
CLI(Command Line Interface)에 액세스	13
공장 기본 사용자 이름 및 암호	13
명령줄 인터페이스 규칙	14
명령 프롬프트	14
명령 구문	15
선택 목록	15
예/아니요 쿼리	15
하위 명령	16
Esc	16
기록	16
명령 완성	16
컨피그레이션 변경	17
범용 CLI 명령	17
컨피그레이션 변경 커밋	17

컨피그레이션 변경 지우기 18
 명령줄 인터페이스 세션 종료 18
 명령줄 인터페이스에서 도움말 찾기 18
 배치 명령 19
 배치 명령의 예 19

장 3 명령: 참조 예제 23
 목록을 읽는 방법 24
 AMP(Advanced Malware Protection) 24
 ampconfig 24
 Usage(사용) 24
 예 25
 파일 평판 및 파일 분석 활성화 25
 파일 분석을 위한 파일 유형 선택 26
 퍼블릭 클라우드 파일 분석 서버를 사용하도록 ESA(Email Security Appliance) 구성 27
 (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성 28
 온프레미스 파일 분석 서버를 사용하도록 ESA(Email Security Appliance) 구성 29
 온프레미스 파일 평판 서버를 사용하도록 ESA(Email Security Appliance) 구성 30
 로컬 파일 평판 캐시 지우기 30
 파일 평판 상태 값에 대한 캐시 만료 기간 구성 31
 파일 회귀 판정 알림 표시 안 함 31
 파일 분석을 위한 Cisco AMP Threat Grid 클러스터링 구성 32
 ampstatus 33
 설명 33
 Usage(사용) 33
 예 34
 Anti-Spam 34
 antispamconfig 34
 설명 34
 Usage(사용) 34
 예 34
 antispamstatus 35

설명	35
Usage(사용)	35
예	35
antispamupdate	36
설명	36
Usage(사용)	36
예	36
incomingrelayconfig	36
설명	36
Usage(사용)	36
예: 수신 릴레이 활성화 수신 릴레이 구성	36
slblconfig	38
설명	38
Usage(사용)	38
배치 형식 - 가져오기	39
Batch Format	39
배치 형식 - 내보내기	39
예 - 허용 목록/차단 목록 항목 가져오기	39
그레이메일 탐지 및 안전한 수신 거부	40
graymailconfig	40
설명	40
Usage(사용)	40
예	40
graymailstatus	41
설명	41
Usage(사용)	41
예	41
graymailupdate	41
설명	41
Usage(사용)	41
예	42
Anti-Virus	42

antivirusconfig	42
설명	42
Usage(사용)	42
예	42
안티바이러스 IDE 세부 사항 보기	43
antivirusstatus	44
설명	44
Usage(사용)	44
예	44
antivirusupdate	44
설명	44
Usage(사용)	44
예	44
명령줄 관리	45
commit	45
설명	45
Usage(사용)	45
예	45
commitdetail	45
설명	45
Usage(사용)	45
예	46
clearchanges 또는 clear	46
설명	46
Usage(사용)	46
예	46
help 또는 h 또는 ?	46
설명	46
Usage(사용)	46
예	46
rollbackconfig	47
Usage(사용)	47

예 47

quit 또는 q 또는 exit 47

 설명 47

 Usage(사용) 47

 예 47

컨피그레이션 파일 관리 48

 loadconfig 48

 설명 48

 Usage(사용) 48

 예 48

 mailconfig 49

 설명 49

 Usage(사용) 49

 예 49

 resetconfig 50

 설명 50

 Usage(사용) 50

 예 50

 saveconfig 51

 설명 51

 Usage(사용) 51

 예 51

 showconfig 51

 설명 51

 Usage(사용) 52

 예 52

외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성 52

 threatfeedconfig 53

 설명 53

 Usage(사용) 53

 예 - 외부 위협 피드 엔진 활성화 53

 예 - 외부 위협 피드 소스 추가 53

threatfeedstatus	54
설명	55
Usage(사용)	55
예 - 외부 위협 피드 엔진의 현재 버전 보기	55
threatfeedupdate	55
설명	55
Usage(사용)	55
예 - 외부 위협 피드 엔진 수동 업데이트	55
클러스터 관리	56
clusterconfig	56
설명	56
Usage(사용)	57
예	57
데이터 유출 방지	58
dlpstatus	58
Usage(사용)	58
예	58
dlpupdate	58
설명	58
Usage(사용)	58
배치 형식	59
예	59
도메인 예외 목록	59
domainrepconfig	59
설명	59
Usage(사용)	59
예	60
S/MIME 보안 서비스	60
smimeconfig	60
설명	60
Usage(사용)	60
예	60

- 도메인 키 62
 - domainkeysconfig 62
 - 설명 62
 - Usage(사용) 62
 - 배치 형식 - 서명 프로필 63
 - 배치 형식 - 확인 프로필 66
 - 배치 형식 - 서명 키 67
 - 배치 형식 - 키 또는 프로필 검색 68
 - 배치 형식 - 전역 설정 69
 - 예: CLI에서 도메인 키 구성 69
 - 샘플 Domain Keys DNS TXT 레코드 생성 71
- DMARC 확인 73
 - dmarcconfig 73
 - 설명 73
 - Usage(사용) 73
 - 배치 형식 - DMARC 확인 프로필 73
 - 예 75
- DNS 77
 - dig 78
 - 설명 78
 - Usage(사용) 78
 - 배치 형식 78
 - 예 79
 - 예: DNSSEC를 지원하는 DNS 서버의 TLSA 레코드 확인 79
 - dnsconfig 80
 - 설명 80
 - Usage(사용) 80
 - 배치 형식 80
 - 예 82
 - dnsflush 84
 - 설명 84
 - Usage(사용) 84

예 84

[dnshostprefs](#) 84

 설명 84

 Usage(사용) 84

 예 85

[dnslistconfig](#) 85

 설명 85

 Usage(사용) 85

 예 85

[dnslisttest](#) 86

 설명 86

 Usage(사용) 86

 예 86

[dnsstatus](#) 86

 설명 86

 Usage(사용) 86

 예 86

[How-Tos 위젯을 사용하여 사용자 경험 향상](#) 87

[howtoupdate](#) 87

 설명 87

 Usage(사용) 87

 예 87

[howtostatus](#) 87

 설명 87

 Usage(사용) 87

 예 88

[일반 관리 및 문제 해결](#) 88

[addressconfig](#) 89

 설명 89

 Usage(사용) 90

 예 90

[adminaccessconfig](#) 90

설명 90
 Usage(사용) 91
 배치 형식 91
 예 - 네트워크 액세스 목록 구성 93
 예 - 로그인 배너 구성 94
 예 - 웹 인터페이스 및 CLI 세션 시간 초과 구성 95

certconfig 96
 설명 96
 Usage(사용) 96
 예 - 인증서에 붙여넣기 96
 예 - 자체 서명 인증서 생성 97
 예 - 자체 서명 S/MIME 서명 인증서 생성 98

날짜 100
 설명 100
 Usage(사용) 100
 예 100

daneverify 100
 설명 100
 Usage(사용) 100
 예 100

진단 101
 설명 101
 diagnostic 명령 사용 101
 Usage(사용) 102
 배치 형식 102
 예: 캐시 표시 및 지우기 103
 예: 다른 메일 서버와의 연결 확인 104
 예: 초기 제조업체 값으로 어플라이언스 컨피그레이션 재설정 104
 서비스 엔진 다시 시작 및 상태 보기 105

diskquotaconfig 106
 Usage(사용) 106

배치 형식	106
예	107
ecconfig	107
Usage(사용)	107
배치 형식	108
예	108
ecstatus	108
Usage(사용)	108
예	108
ecupdate	108
Usage(사용)	109
배치 형식	109
예	109
encryptionconfig	109
Usage(사용)	109
예	109
encryptionstatus	112
설명	112
Usage(사용)	112
예	112
encryptionupdate	112
설명	112
Usage(사용)	112
예	113
enginestatus	113
설명	113
Usage(사용)	113
예	113
featurekey	114
설명	114
Usage(사용)	114
예	114

featurekeyconfig 115

- 설명 115
- Usage(사용) 115
- 예 115

generalconfig 115

- 설명 115
- Usage(사용) 115
- 예 - Internet Explorer 호환성 모드 재정의 구성 116

healthcheck 116

- 설명 116
- Usage(사용) 116
- 예 116

healthconfig 117

- 설명 117
- Usage(사용) 117
- 예 117

ntpconfig 118

- 설명 118
- Usage(사용) 118
- 예 118

portalregistrationconfig 119

- Usage(사용) 119
- 예 119

reboot 120

- 설명 120
- Usage(사용) 120
- 예 120

repengstatus 120

- 설명 120
- Usage(사용) 120
- 예 120

resume 120

설명	120
Usage(사용)	121
예	121
resumedel	121
설명	121
Usage(사용)	121
예	121
resumelistener	121
설명	121
Usage(사용)	121
예	122
회선	122
설명	122
Usage(사용)	122
예	122
settime	123
설명	123
Usage(사용)	123
예	123
settz	123
설명	123
Usage(사용)	123
예	123
shutdown	124
설명	124
Usage(사용)	124
예	124
smaconfig	124
설명	125
Usage(사용)	125
예	125
sshconfig	125

[설명](#) 125
[Usage\(사용\)](#) 126
[예](#) 126
[status](#) 129
 [설명](#) 129
 [Usage\(사용\)](#) 129
 [예](#) 129
[supportrequest](#) 130
 [설명](#) 130
 [Usage\(사용\)](#) 130
 [예](#) 130
[supportrequeststatus](#) 132
 [설명](#) 132
 [Usage\(사용\)](#) 132
 [예](#) 132
[supportrequestupdate](#) 132
 [설명](#) 132
 [Usage\(사용\)](#) 132
 [예](#) 132
[suspend](#) 132
 [설명](#) 132
 [Usage\(사용\)](#) 132
 [예](#) 133
[suspenddel](#) 133
 [설명](#) 133
 [Usage\(사용\)](#) 133
 [예](#) 133
[suspendlistener](#) 133
 [설명](#) 133
 [Usage\(사용\)](#) 133
 [예](#) 134
[tcp services](#) 134

설명	134
Usage(사용)	134
예	134
techsupport	135
설명	135
Usage(사용)	135
예	135
tlsverify	136
설명	136
Usage(사용)	136
배치 형식	136
예	136
trace	136
설명	136
Usage(사용)	137
예	137
trackingconfig	138
설명	138
Usage(사용)	138
예	138
tzupdate	139
설명	139
Usage(사용)	139
배치 형식	139
예	139
updateconfig	139
설명	139
Usage(사용)	139
예	140
updatenow	143
설명	143
Usage(사용)	143

- 배치 형식 143
 - 예 144
- 버전 144
 - 설명 144
 - Usage(사용) 144
 - 예 144
- wipedata 144
 - 설명 144
 - Usage(사용) 145
 - 예 145
- upgrade 145
 - 설명 145
 - Usage(사용) 145
 - 예 145
- 콘텐츠 스캔 146
 - contentscannerstatus 146
 - Usage(사용) 146
 - 예 146
 - contentscannerupdate 146
 - Usage(사용) 146
 - 예 146
- LDAP 146
 - ldapconfig 147
 - 설명 147
 - Usage(사용) 147
 - 예 - 새 LDAP 서버 프로파일 생성 147
 - 예 - 전역 설정 구성 150
 - ldapflush 151
 - 설명 151
 - Usage(사용) 151
 - 예 151
 - ldaptest 151

설명	151
Usage(사용)	151
예	151
sievechar	152
설명	152
Usage(사용)	152
예	152
메일 전달 컨피그레이션/모니터링	153
addresslistconfig	153
설명	153
Usage(사용)	153
배치 형식	154
예	154
aliasconfig	155
설명	155
Usage(사용)	155
배치 형식	155
예	156
archivemessage	157
설명	157
Usage(사용)	157
예	158
altsrchoost	158
설명	158
Usage(사용)	158
예	158
bounceconfig	159
설명	159
Usage(사용)	159
예	160
리스너에 바운스 프로필 적용	161
bouncerecipients	162

[설명](#) **162**
[Usage\(사용\)](#) **162**
[예](#) **162**
bvconfig **163**
[설명](#) **163**
[Usage\(사용\)](#) **163**
[예](#) **164**
deleterecipients **164**
[설명](#) **164**
[Usage\(사용\)](#) **165**
[예](#) **165**
[모두 삭제](#) **165**
deliveryconfig **166**
[설명](#) **166**
[Usage\(사용\)](#) **166**
[예](#) **166**
delivernow **166**
[설명](#) **166**
[Usage\(사용\)](#) **166**
[예](#) **167**
destconfig **167**
[destconfig 명령 사용](#) **167**
[샘플 목적지 제어 테이블](#) **168**
[배치 형식](#) **168**
[예: 새 destconfig 항목 생성](#) **170**
[예: 바운스 프로파일 및 TLS 설정](#) **171**
[예: 인바운드 “완충제”](#) **172**
[예: 전역 설정](#) **173**
[예: DANE 지원을 사용하여 TLS 연결 활성화](#) **174**
hostrate **175**
[설명](#) **175**
[Usage\(사용\)](#) **175**

예 175

hoststatus 175

 설명 175

 Usage(사용) 175

 예 176

imageanalysisconfig 177

 설명 177

 Usage(사용) 177

 예 177

oldmessage 178

 설명 178

 Usage(사용) 178

 예 178

rate 178

 설명 178

 Usage(사용) 178

 예 178

redirectrecipients 179

 설명 179

 Usage(사용) 179

 배치 형식 179

 예 179

resetcounters 180

 설명 180

 Usage(사용) 180

 예 180

removemessage 180

 설명 180

 Usage(사용) 180

 예 180

showmessage 181

 설명 181

Usage(사용) 181
 예 181

showrecipients 181
 설명 181
 Usage(사용) 181
 배치 형식 181
 예 182

status 183
 Usage(사용) 183
 예 183

tophosts 184
 설명 184
 Usage(사용) 184
 예 184

topin 184
 설명 184
 Usage(사용) 184
 예 185

unsubscribe 185
 설명 185
 Usage(사용) 185
 예 185

workqueue 186
 설명 186
 Usage(사용) 186
 예 186

네트워크 컨피그레이션/네트워크 툴 187

etherconfig 187
 설명 187
 Usage(사용) 188
 예 188

interfaceconfig 189

설명	189
Usage(사용)	189
배치 형식	189
예: 인터페이스 구성	190
nslookup	191
설명	191
Usage(사용)	192
예	192
netstat	192
설명	192
Usage(사용)	192
예	192
packetcapture	193
설명	193
Usage(사용)	193
예	193
ping	194
설명	194
Usage(사용)	194
예	195
ping6	195
설명	195
Usage(사용)	195
예	196
routeconfig	196
설명	196
Usage(사용)	196
배치 형식	197
예	197
setgateway	198
설명	198
Usage(사용)	198

예	199
sethostname	199
설명	199
Usage(사용)	199
예	199
smtproutes	200
설명	200
Usage(사용)	200
배치 형식	200
예	200
sslconfig	201
설명	201
Usage(사용)	201
예	202
sslv3config	204
설명	204
Usage(사용)	204
예	204
telnet	204
설명	204
Usage(사용)	204
예	205
traceroute	205
설명	205
Usage(사용)	205
예	205
traceroute6	206
설명	206
Usage(사용)	206
예	206
신종 바이러스 필터(Outbreak Filter)	206
outbreakconfig	207

설명	207
Usage(사용)	207
예	207
outbreakflush	208
설명	208
Usage(사용)	208
예	208
outbreakstatus	208
설명	208
Usage(사용)	208
예	208
outbreakupdate	209
설명	209
Usage(사용)	209
예	209
정책 시행	209
dictionaryconfig	210
설명	210
Usage(사용)	210
예	210
exceptionconfig	213
설명	213
Usage(사용)	213
예	213
filters	214
설명	214
Usage(사용)	214
예	214
policyconfig	216
설명	216
Usage(사용)	216
예	216

quarantineconfig	238
설명	238
Usage(사용)	238
예	238
사용자와 격리	239
scanconfig	239
설명	239
Usage(사용)	239
예	239
예: 스캔할 수 없는 메시지에 대한 메시지 처리 작업 구성	241
stripheaders	242
설명	242
Usage(사용)	242
예	243
textconfig	243
설명	243
Usage(사용)	243
예	243
텍스트 리소스 가져오기	244
텍스트 리소스 내보내기	245
로깅 및 알림	246
alertconfig	246
설명	246
Usage(사용)	246
예: 새 알림 생성	246
displayalerts	247
설명	247
Usage(사용)	247
예	247
findevent	248
설명	248
Usage(사용)	248

예: envelope FROM 기준 검색 248

예: 메시지 ID 기준 검색 248

예: 제목 기준 검색 249

예: envelope TO 기준 검색 249

grep 250

 설명 250

 Usage(사용) 250

 grep의 예 251

logconfig 251

 설명 251

 Usage(사용) 251

 FTP 푸시 로그 서브스크립션의 예 251

 SCP 푸시 로그 서브스크립션의 예 253

 Syslog 푸시 로그 서브스크립션의 예 256

rollovernow 257

 설명 257

 Usage(사용) 257

 예 258

snmpconfig 258

 설명 258

 Usage(사용) 258

 예 258

tail 260

 설명 260

 Usage(사용) 260

 예 260

보고 261

 reportingconfig 261

 reportingconfig 명령 사용 261

 Usage(사용) 261

 예: 보고 필터 활성화(M Series만) 261

 도메인 보고서에 대한 HAT REJECT 정보 활성화(M Series만) 262

시간 초과 알림 활성화(M Series만) 262

Email Security Appliance에 대한 중앙 집중식 보고 활성화 263

데이터 보고용 스토리지 제한 구성(C-Series만) 263

Senderbase 264

 sbstatus 264

 설명 264

 Usage(사용) 264

 예 264

 senderbaseconfig 264

 설명 264

 Usage(사용) 264

 예 265

발신자 도메인 평판 필터링 265

 sdrconfig 265

 설명 265

 Usage(사용) 265

 예 266

 sdradvancedconfig 266

 설명 266

 Usage(사용) 267

 예 267

 sdrstatus 267

 설명 267

 Usage(사용) 267

 예 267

 sdrupdate 268

 설명 268

 Usage(사용) 268

 예 268

 sdrdiagnostics 268

 설명 268

 Usage(사용) 268

예	269
Smart Software Licensing	269
license_smart	269
설명	269
Usage(사용)	269
예: Smart Agent 서비스용 포트 구성	270
예: Smart Licensing 활성화	270
예: Smart Software Manager에 어플라이언스 등록	270
예: Smart Licensing의 상태	270
예: Smart Licensing의 상태 요약	271
예: Smart Transport URL 설정	271
예: 라이선스 요청	272
예: 라이선스 해제	272
show_license	272
설명	273
예: Smart Licensing의 상태	273
예: Smart Licensing의 상태 요약	273
SMTP 서비스 컨피그레이션	273
callaheadconfig	273
설명	273
Usage(사용)	274
예	274
listenerconfig	275
설명	275
Usage(사용)	276
배치 형 - 일반 listenerconfig	276
배치 형식 - HAT	276
배치 형식 - RAT	281
예 - 리스너 추가	282
예 - 발신자 그룹에 발신자의 발신지 국가 추가	283
예 - 내보내기 및 가져오기를 통해 리스너에 대한 HAT(Host Access Table) 사용자 정의	287
예 - 공개 키 수집 및 S/MIME 해독/확인 활성화	293

Example - 고급 HAT 매개변수 296

listenerconfig에 bypass_ca 인수 추가 298

예 - SPF 및 SIDF 구성 298

예: SPF/SIDF 설정 300

예: 기본 정책 매개변수의 SPF/SIDF 301

예 - DMARC 확인 활성화 301

localeconfig 305

설명 305

Usage(사용) 305

예 305

smtpauthconfig 306

설명 306

Usage(사용) 306

예 306

시스템 설치 307

systemsetup 307

설명 307

Usage(사용) 307

예 308

URL 필터링 310

aggregatorconfig 311

설명 311

Usage(사용) 311

예 311

urllistconfig 311

설명 311

Usage(사용) 311

예 311

webcacheflush 312

설명 312

Usage(사용) 312

예 312

- websecurityadvancedconfig 313
 - 설명 313
 - Usage(사용) 313
 - 배치 형식 313
 - 예 313
 - 예: 단축 URL에 대한 URL 필터링 활성화 313
 - 예: 메시지 첨부 파일의 URL에 대한 스캔 제한 구성 314
- websecurityconfig 315
 - 설명 315
 - Usage(사용) 315
 - 예 315
- websecuritydiagnostics 316
 - 설명 316
 - Usage(사용) 316
 - 예 316
- 사용자 관리 316
 - userconfig 316
 - 설명 316
 - Usage(사용) 316
 - 예 - 새 사용자 계정 생성 317
 - 예 - 외부 인증을 위한 RADIUS 서버 설정 318
 - 예: 특정 사용자 역할에 대한 이중 인증 활성화 319
 - passphrase 또는 passwd 321
 - 설명 321
 - Usage(사용) 321
 - 예 321
 - last 322
 - 설명 322
 - Usage(사용) 322
 - 예 322
 - who 322
 - 설명 322

Usage(사용) 322
 예 322

whoami 323
 설명 323
 Usage(사용) 323
 예 323

가상 어플라이언스 관리 323
 loadlicense 323
 설명 323
 Usage(사용) 323
 예 324

showlicense 324
 설명 324
 Usage(사용) 324
 배치 형식 324
 예 324

지리위치 325
 geolocationupdate 325
 설명 325
 Usage(사용) 325
 예 325

geolocationstatus 325
 설명 325
 Usage(사용) 325
 예 326



서론

이 책의 지침은 네트워킹 및 이메일 관리에 대한 지식이 있는 숙련된 시스템 관리자를 위해 마련되었습니다.

이 장에는 다음 섹션이 포함되어 있습니다.

- 이 책을 읽기 전에, xxxiii 페이지
- 표기 규칙, xxxiii 페이지
- 추가 리소스, xxxiv 페이지

이 책을 읽기 전에



참고 이미 네트워크에 어플라이언스를 연결한 경우 어플라이언스의 기본 IP 주소가 네트워크의 다른 IP 주소와 충돌하지 않아야 합니다. 출고 시 관리 포트에 할당된 IP 주소는 192.168.42.42입니다. 어플라이언스에 IP 주소를 지정하는 것에 대한 자세한 내용은 해당 릴리스 사용 설명서의 "설정 및 설치" 장을 참조하십시오.

표기 규칙

다음 표에서는 표기 규칙을 보여 줍니다.

서체 또는 기호	의미	예
AaBbCc123	명령, 파일, 디렉터리의 이름 또는 컴퓨터 화면 출력	Please choose an IP interface for this Listener. sethostname 명령은 어플라이언스의 이름을 설정합니다.

서체 또는 기호	의미	예
AaBbCc123	컴퓨터 화면 출력과 대비되는 사용자 입력 내용	<pre>mail3.example.com> commit Please enter some comments describing your changes: []> Changed the system hostname</pre>
<i>AaBbCc123</i>	책 제목, 새로운 단어나 용어, 강조할 단어. 실제 이름 또는 값으로 대체되는 명령행 변수	<p>빠른 시작 가이드를 참고하십시오.</p> <p>어플라이언스에서는 발신 패킷을 보내기 위해 고유하게 인터페이스를 선택할 수 있어야 합니다.</p> <pre>Before you begin, please reset your passphrase to a new value. Old passphrase: ironport New passphrase: <i>your_new_passphrase</i></pre> <p>새 암호 다시 입력: <i>your_new_passphrase</i></p>

추가 리소스

설명서

다음 사이트에서 Email Security Appliance 설명서를 구할 수 있습니다.

<http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html>

기술 자료

Cisco Content Security 제품에 대한 정보를 제공하는 기술 자료는 다음 사이트에서 액세스하십시오.

<http://www.cisco.com/web/ironport/knowledgebase.html>

Cisco.com 사용자 ID가 있어야 사이트에 액세스할 수 있습니다. Cisco.com 사용자 ID가 없는 경우 Cisco 어카운트 등록을 참고하십시오.

Cisco Support Community

Cisco 지원 커뮤니티는 Cisco 고객, 파트너, 직원을 위한 온라인 포럼입니다. 여기서 일반적인 콘텐츠 보안 문제에 대해 논의하고 특정 Cisco 제품에 대한 기술 정보를 얻을 수 있습니다. 포럼에 주제를 게시하여 궁금한 점을 질문하고 다른 사용자와 정보를 공유할 수 있습니다.

다음 사이트에서 Cisco Email Security Appliances 지원 커뮤니티에 액세스하십시오.

<https://supportforums.cisco.com/community/netpro/security/email>

고객 지원

다음 방법을 사용하여 지원을 받을 수 있습니다.

미국: 전화 1 (408) 526-7209 또는 무료 전화 1 (800) 553-2447

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

지원 사이트: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

리셀러 또는 다른 공급자를 통해 지원을 구매한 경우 제품 지원 문제는 해당 공급자에게 직접 문의해 주십시오.

Cisco 계정 등록

Cisco.com의 많은 리소스에 액세스하려면 Cisco 계정이 필요합니다.

Cisco.com 사용자 ID가 없는 경우 다음에서 등록할 수 있습니다.

<https://tools.cisco.com/RPF/register/register.do%20>

Cisco에 의견 보내기

기술 출판 팀은 더 우수한 제품 설명서를 제공하기 위해 최선을 다하고 있습니다. 소중한 의견과 제안을 언제든지 보내주십시오. 다음 이메일 주소로 의견을 보내실 수 있습니다.

contentsecuritydocs@cisco.com

메시지의 제목에 이 책의 제목 및 제목 페이지에 표시된 발행일을 기재해 주십시오.



1 장

CLI 빠른 참조 설명서

이 장에는 다음 섹션이 포함되어 있습니다.

알맞은 CLI 명령, 간략한 설명, C Series, X Series, M Series 플랫폼에서 사용 가능 여부를 확인하려면 이 표를 사용하십시오.

- CLI 명령(커밋 불필요), 1 페이지
- CLI 명령(커밋 필요), 7 페이지

CLI 명령(커밋 불필요)

CLI 명령	설명	사용 가능 플랫폼
ampstatus , 33 페이지	다양한 파일 평판 및 분석 구성 요소의 버전을 표시합니다.	C Series, X Series
antispamstatus , 35 페이지	안티스팸 상태 표시	C Series, X Series
antispamupdate , 36 페이지	스팸 정의 수동 업데이트	C Series, X Series
antivirusstatus , 44 페이지	안티바이러스 상태 표시	C Series, X Series
antivirusupdate , 44 페이지	바이러스 정의 수동 업데이트	C Series, X Series
archivemessage , 157 페이지	큐의 오래된 메시지 아카이빙	C Series, X Series
bouncerecipients , 162 페이지	큐의 메시지 바운스	C Series, X Series, M Series
clearchanges 또는 clear , 46 페이지	변경 지우기	C Series, X Series, M Series

CLI 명령	설명	사용 가능 플랫폼
commit, 45 페이지	변경 커밋	C Series, X Series, M Series
commitdetail, 45 페이지	마지막 커밋에 대한 세부 정보 표시	C Series, X Series
contentscannerstatus, 146 페이지	콘텐츠 스캐너 버전 정보를 표시합니다.	C Series, X Series
contentscannerupdate, 146 페이지	콘텐츠 스캐너 엔진의 수동 업데이트를 요청합니다.	C Series, X Series
날짜, 100 페이지	현재 날짜 및 시간 표시	C Series, X Series, M Series
daneverify, 100 페이지	지정된 도메인에 대해 DANE가 지원되는지 여부를 확인합니다.	C Series, X Series
deleterecipients, 164 페이지	큐에서 메시지 삭제	C Series, X Series, M Series
delivernow, 166 페이지	즉시 전송하기 위해 메시지 일정 조정	C Series, X Series, M Series
진단, 101 페이지	RAID 디스크, 네트워크 캐시, SMTP 연결 확인. 네트워크 캐시 지우기	C Series, X Series, M Series
dig, 78 페이지	DNS 서버의 레코드 조회	C Series, X Series
displayalerts, 247 페이지	어플라이언스에서 마지막으로 전송된 n개 알림 표시	C Series, X Series, M Series
dlpstatus, 58 페이지	DLP 엔진의 버전 정보	C Series, X Series
dlpupdate, 58 페이지	DLP 엔진 업데이트	C Series, X Series
dnsflush, 84 페이지	DNS 캐시의 모든 항목 지우기	C Series, X Series, M Series
dnslisttest, 86 페이지	DNS 기반 목록 서비스를 위한 DNS 조회 테스트	C Series, X Series
dnsstatus, 86 페이지	DNS 통계 표시	C Series, X Series, M Series
domainreconfig, 59 페이지	도메인 예외 목록 생성	C Series, X Series
ecstatus, 108 페이지	인증서 취득에 사용되는 등록 클라이언트의 버전 확인	C Series
ecupdate, 108 페이지	인증서 취득에 사용되는 등록 클라이언트 업데이트	C Series

CLI 명령	설명	사용 가능 플랫폼
encryptionstatus, 112 페이지	PXE 엔진 및 도메인 매핑 파일의 버전 표시	C Series, X Series
encryptionupdate, 112 페이지	PXE 엔진에 대한 업데이트 요청	C Series, X Series
enginestatus, 113 페이지	어플라이언스에서 활성화된 모든 엔진의 상태 및 CPU 사용량을 표시합니다.	C Series, X Series
featurekey, 114 페이지	시스템 기능 키 관리	C Series, X Series, M Series
findevent, 248 페이지	메일 로그 파일에서 이벤트 찾기	C Series, X Series, M Series
geolocationupdate, 325 페이지	지리위치 목록을 수동으로 업데이트합니다.	C Series, X Series
geolocationstatus, 325 페이지	지리위치 목록의 현재 버전을 표시합니다.	C Series, X Series
howtoupdate, 87 페이지	How-Tos 구성 요소 수동 업데이트	C Series, X Series
howtostatus, 87 페이지	How-Tos 구성 요소의 현재 버전 표시	C Series, X Series
graymailstatus, 41 페이지	기존 그레이메일 규칙의 세부사항 표시	C Series, X Series
graymailupdate, 41 페이지	그레이메일 규칙 수동 업데이트	C Series, X Series
grep, 250 페이지	로그 파일에서 텍스트 검색	C Series, X Series, M Series
healthcheck, 116 페이지	Email Security Appliance 상태 확인	C Series, X Series
help 또는 h 또는 ?, 46 페이지	도움말	C Series, X Series, M Series
hostrate, 175 페이지	특정 호스트의 활동 모니터링	C Series, X Series, M Series
hoststatus, 175 페이지	해당 호스트 이름의 상태 확인	C Series, X Series, M Series
last, 322 페이지	시스템에 최근에 로그인한 사람 표시	C Series, X Series, M Series
ldapflush, 151 페이지	캐싱된 LDAP 결과 플러시	C Series, X Series
ldaptest, 151 페이지	단일 LDAP 쿼리 테스트 수행	C Series, X Series
loadlicense, 323 페이지	가상 어플라이언스 라이선스 로드	모든 가상 어플라이언스

CLI 명령	설명	사용 가능 플랫폼
mailconfig, 49 페이지	이메일 주소에 현재 컨피그레이션 전송	C Series, X Series, M Series
nslookup, 191 페이지	이름 서버 쿼리	C Series, X Series, M Series
netstat, 192 페이지	네트워크 연결, 라우팅 테이블, 네트워크 인터페이스 통계 표시	C Series, X Series, M Series
outbreakflush, 208 페이지	캐싱된 보안 침해 규칙 지우기	C Series, X Series
outbreakstatus, 208 페이지	현재 보안 침해 규칙 표시	C Series, X Series
outbreakupdate, 209 페이지	보안 침해 필터 규칙 업데이트	C Series, X Series
oldmessage, 178 페이지	큐에서 오래된 메시지의 목록 표시	C Series, X Series
packetcapture, 193 페이지	네트워크를 통해 전송되거나 수신되는 패킷 인터셉트 및 표시	C Series, X Series, M Series
passphrase 또는 passwd, 321 페이지	암호 변경	C Series, X Series, M Series
ping, 194 페이지	네트워크 호스트 ping	C Series, X Series, M Series
ping6, 195 페이지	IPV6를 사용하여 네트워크 호스트 ping	C Series, X Series, M Series
quit 또는 q 또는 exit, 47 페이지	종료	C Series, X Series, M Series
rate, 178 페이지	메시지 처리량 모니터링	C Series, X Series, M Series
reboot, 120 페이지	시스템 다시 시작	C Series, X Series, M Series
redirectrecipients, 179 페이지	다른 릴레이 호스트에 모든 메시지 리디렉션	C Series, X Series
removemessage, 180 페이지	큐에서 전달되지 않은 오래된 메시지 제거	C Series, X Series
repengstatus, 120 페이지	평판 엔진의 버전 정보 요청	C Series, X Series, M Series
resetconfig, 50 페이지	공장 기본 컨피그레이션 복원	C Series, X Series, M Series
resetcounters, 180 페이지	시스템의 모든 카운터 재설정	C Series, X Series, M Series
resume, 120 페이지	수신 및 전달 다시 시작	C Series, X Series, M Series

CLI 명령	설명	사용 가능 플랫폼
resumedel, 121 페이지	전달 다시 시작	C Series, X Series, M Series
resumelister, 121 페이지	수신 다시 시작	C Series, X Series, M Series
회선, 122 페이지	이전 릴리스로 되돌리기	C Series, X Series, M Series
rollovernow, 257 페이지	로그 파일 롤오버	C Series, X Series, M Series
saveconfig, 51 페이지	디스크에 컨피그레이션 저장	C Series, X Series, M Series
sbstatus, 264 페이지	SenderBase 쿼리의 상태 표시	C Series, X Series
sdrstatus, 267 페이지	SDR 구성 요소의 현재 버전 표시	C Series, X Series
sdrupdate, 268 페이지	SDR 구성 요소 수동 업데이트	C Series, X Series
sdrdiagnostics, 268 페이지	Cisco Email Security 게이트웨이가 SDR 서비스에 연결되어 있는지 확인	C Series, X Series
settime, 123 페이지	시스템 시계 수동 설정	C Series, X Series, M Series
showmessage, 181 페이지	큐에서 전달되지 않은 오래된 메시지 표시	C Series, X Series
showconfig, 51 페이지	모든 컨피그레이션 값 표시	C Series, X Series, M Series
showlicense, 324 페이지	가상 어플라이언스 라이선스 정보 표시	모든 가상 어플라이언스
show_license, 272 페이지	Smart Licensing 상태 및 상태 요약 표시합니다.	C Series, X Series, M Series
showrecipients, 181 페이지	큐의 메시지를 수신자 호스트 기준, Envelope From 주소 기준으로 또는 모두 표시	C Series, X Series
shutdown, 124 페이지	전원을 끄기 위해 시스템 종료	C Series, X Series, M Series
slblconfig, 38 페이지	허용 목록/차단 목록 설정 구성	C Series, X Series
status, 129 페이지	시스템 상태	C Series, X Series, M Series
supportrequest, 130 페이지	Cisco TAC에 메시지 전송	C Series, X Series, M Series
supportrequeststatus, 132 페이지	지원 요청 키워드 버전 정보 표시	C Series, X Series, M Series

CLI 명령	설명	사용 가능 플랫폼
supportrequestupdate, 132 페이지	지원 요청 키워드에 대한 수동 업데이트 요청	C Series, X Series, M Series
suspend, 132 페이지	수신 및 전달 일시 중단	C Series, X Series, M Series
suspenddel, 133 페이지	전달 일시 중단	C Series, X Series, M Series
suspendlistener, 133 페이지	수신 일시 중단	C Series, X Series, M Series
systemsetup, 307 페이지	최초 시스템 설정	C Series, X Series
tail, 260 페이지	지속적으로 로그 파일의 끝 표시	C Series, X Series, M Series
techsupport, 135 페이지	Cisco TAC에서 시스템에 액세스하도록 허용	C Series, X Series, M Series
telnet, 204 페이지	원격 호스트에 연결	C Series, X Series, M Series
threatfeedstatus, 54 페이지	ETF 엔진의 현재 버전 표시	C Series, X Series
threatfeedupdate, 55 페이지	ETF 엔진 수동 업데이트	C Series, X Series
tlsverify, 136 페이지	원격 호스트에 아웃바운드 TLS 연결 설정 및 모든 TLS 연결 문제 디버깅	C Series, X Series
tophosts, 184 페이지	큐 크기 기준으로 최상위 호스트 표시	C Series, X Series, M Series
topin, 184 페이지	수신 연결 수를 기준으로 최상위 호스트 표시	C Series, X Series, M Series
trace, 136 페이지	시스템을 지나는 메시지의 플로우 추적	C Series, X Series, M Series
traceroute, 205 페이지	원격 호스트에 대한 네트워크 경로 표시	C Series, X Series, M Series
traceroute6, 206 페이지	IPv6를 사용하여 원격 호스트에 대한 네트워크 경로 표시	C Series, X Series, M Series
tzupdate, 139 페이지	표준 시간대 규칙 업데이트	C Series, X Series, M Series
updatenow, 143 페이지	모든 구성 요소 업데이트	C Series, X Series, M Series
upgrade, 145 페이지	업그레이드 설치	C Series, X Series, M Series
버전, 144 페이지	시스템 버전 정보 표시	C Series, X Series, M Series

CLI 명령	설명	사용 가능 플랫폼
wipedata, 144 페이지	디스크의 코어 파일 지우기, 최신 코어덤프 작업의 상태 확인	C Series, X Series, M Series
webcacheflush, 312 페이지	URL 필터링 기능에서 사용하는 캐시 플러시	C Series, X Series, M Series
websecuritydiagnostics, 316 페이지	URL 필터링의 진단 통계 보기	C Series, X Series, M Series
who, 322 페이지	로그인한 사람 나열	C Series, X Series, M Series
whoami, 323 페이지	현재 사용자 ID 표시	C Series, X Series, M Series
workqueue, 186 페이지	작업 큐 일시 중지 상태 표시 또는 변경	C Series, X Series

CLI 명령(커밋 필요)

CLI 명령	설명	사용 가능 플랫폼
addressconfig, 89 페이지	시스템에서 생성한 메일의 발신자 주소 구성	C Series, X Series, M Series
addresslistconfig, 153 페이지	주소 목록 구성	C Series, X Series
adminaccessconfig, 90 페이지	네트워크 액세스 목록 및 배너 로그인 구성	C Series, X Series
aggregatorconfig, 311 페이지	Cisco Aggregator Server의 주소 구성	C Series, X Series
alertconfig, 246 페이지	이메일 알림 구성	C Series, X Series, M Series
aliasconfig, 155 페이지	이메일 별칭 구성	C Series, X Series
altsrchostr, 158 페이지	Virtual Gateway™ 매핑 구성	C Series, X Series
amconfig, 24 페이지	Advanced Malware Protection(파일 평판 및 분석) 구성	C Series, X Series, M Series
antispamconfig, 34 페이지	안티스팸 정책 구성	C Series, X Series
antivirusconfig, 42 페이지	안티바이러스 정책 구성	C Series, X Series

CLI 명령	설명	사용 가능 플랫폼
bounceconfig, 159 페이지	바운스 동작 구성	C Series, X Series, M Series
bvconfig, 163 페이지	발신 메일의 주요 설정 구성, 잘못된 바운스의 처리 방법 구성	C Series, X Series
callaheadconfig, 273 페이지	SMTP Call-Ahead 프로파일 추가, 수정, 삭제	C Series, X Series, M Series
certconfig, 96 페이지	보안 인증서 및 키 구성	C Series, X Series, M Series
clusterconfig, 56 페이지	클러스터 관련 설정 구성	C Series, X Series
deliveryconfig, 166 페이지	메일 전달 구성	C Series, X Series
destconfig, 167 페이지	목적지 제어 테이블의 옵션 구성	C Series, X Series
dictionaryconfig, 210 페이지	콘텐츠 사전 구성	C Series, X Series, M Series
diskquotaconfig, 106 페이지	디스크 공간 구성	C Series, X Series, M Series
dmarcconfig, 73 페이지	DMARC 설정 구성	C Series, X Series
dnsconfig, 80 페이지	DNS 설정 구성	C Series, X Series
dnshostprefs, 84 페이지	IPv4/IPv6 DNS 기본 설정 구성	C Series, X Series, M Series
dnslistconfig, 85 페이지	DNS 목록 서비스 지원 구성	C Series, X Series
domainkeysconfig, 62 페이지	DomainKeys 지원 구성	C Series, X Series
ecconfig, 107 페이지	인증서 취득에 사용되는 등록 클라이언트 구성	C Series, X Series, M Series
encryptionconfig, 109 페이지	이메일 암호화 구성	C Series, X Series
etherconfig, 187 페이지	이더넷 설정 구성	C Series, X Series, M Series

CLI 명령	설명	사용 가능 플랫폼
exceptionconfig, 213 페이지	도메인 예외 테이블 구성	C Series, X Series
featurekeyconfig, 115 페이지	기능 키 자동 확인 및 업데이트	C Series, X Series, M Series
filters, 214 페이지	메시지 처리 옵션 구성	C Series, X Series
generalconfig, 115 페이지	브라우저 설정 및 기타 일반 설정 구성	C Series, X Series, M Series
graymailconfig, 40 페이지	그레이메일 탐지 및 안전 수신 거부의 전역 설정 구성	C Series, X Series
healthconfig, 117 페이지	어플라이언스의 다양한 상태 매개변수 임계값 구성	C Series, X Series, M Series
imageanalysisconfig, 177 페이지	IronPort 이미지 분석 설정 구성	C Series, X Series, M Series
incomingrelayconfig, 36 페이지	수신 릴레이 구성	C Series, X Series
interfaceconfig, 189 페이지	이더넷 IP 주소 구성	C Series, X Series, M Series
ldapconfig, 147 페이지	LDAP 서버 구성	C Series, X Series
license_smart, 269 페이지	Smart Software Licensing 기능을 구성합니다.	C Series, X Series, M Series
listenerconfig, 275 페이지	메일 리스너 구성	C Series, X Series
loadconfig, 48 페이지	컨피그레이션 파일 로드	C Series, X Series, M Series
localeconfig, 305 페이지	다국어 설정 구성	C Series, X Series
logconfig, 251 페이지	로그 파일에 대한 액세스 구성	C Series, X Series, M Series
ntpconfig, 118 페이지	NTP 시간 서버 구성	C Series, X Series, M Series
outbreakconfig, 207 페이지	보안 침해 필터 구성	C Series, X Series
policyconfig, 216 페이지	수신자 또는 발신자 기반 정책에 따라 구성	C Series, X Series

CLI 명령	설명	사용 가능 플랫폼
portalregistrationconfig, 119 페이지	어플라이언스에 대한 스팸 전송 추적 포털 등록 ID를 설정합니다.	C Series, X Series
quarantineconfig, 238 페이지	시스템 격리 구성	C Series, X Series
reportingconfig, 261 페이지	보고 설정 구성	C Series, X Series, M Series
rollbackconfig, 47 페이지	이전에 커밋한 컨피그레이션 중 하나로 롤백	C Series, X Series, M Series
routeconfig, 196 페이지	IP 라우팅 테이블 구성	C Series, X Series, M Series
scanconfig, 239 페이지	첨부 파일 검사 정책 구성	C Series, X Series
sdrconfig, 265 페이지	Cisco Email Security 게이트웨이에서 SDR 필터링 활성화 및 구성	C Series, X Series
sdradvancedconfig, 266 페이지	SDR 서비스에 Cisco Email Security 게이트웨이를 연결할 때 고급 파라미터 구성	C Series, X Series
senderbaseconfig, 264 페이지	SenderBase 연결 설정 구성	C Series, X Series
setgateway, 198 페이지	기본 게이트웨이(라우터) 설정	C Series, X Series, M Series
sethostname, 199 페이지	시스템 이름 설정	C Series, X Series, M Series
settz, 123 페이지	현지 표준 시간대 설정	C Series, X Series, M Series
sievechar, 152 페이지	RFC 3598에 따라 Sieve 이메일 필터링을 위한 문자 구성	C Series, X Series
smimeconfig, 60 페이지	S/MIME 기능 구성	C Series, X Series, M Series
smtpauthconfig, 306 페이지	SMTP Auto 프로파일 구성	C Series, X Series
smtproutes, 200 페이지	영구 도메인 리디렉션 설정	C Series, X Series, M Series
snmpconfig, 258 페이지	SNMP 구성	C Series, X Series, M Series
sshconfig, 125 페이지	SSH 키 구성	C Series, X Series, M Series
sslconfig, 201 페이지	SSL 설정 구성	C Series, X Series, M Series

CLI 명령	설명	사용 가능 플랫폼
sslv3config, 204 페이지	SSLv3 활성화/비활성화	C Series, X Series, M Series
stripheaders, 242 페이지	제거할 메시지 헤더 설정	C Series, X Series
tcpservices, 134 페이지	프로세스에서 여는 파일에 대한 정보 표시	C Series, X Series, M Series
textconfig, 243 페이지	텍스트 리소스 구성	C Series, X Series
threatfeedconfig, 53 페이지	Cisco Email Security 게이트웨이에서 ETF 엔진 활성화 및 구성	C Series, X Series
trackingconfig, 138 페이지	추적 시스템 구성	C Series, X Series, M Series
unsubscribe, 185 페이지	전역 수신 거부 목록 업데이트	C Series, X Series, M Series
updateconfig, 139 페이지	시스템 업데이트 매개변수 구성	C Series, X Series
LDAP, 146 페이지	시스템 업데이트 매개변수 구성(사용 중지된 명령)	
urllistconfig, 311 페이지	안전한 URL의 화이트리스트 구성	C Series, X Series, M Series
userconfig, 316 페이지	사용자 계정 및 외부 인증 소스와의 연결 관리	C Series, X Series, M Series
websecurityadvancedconfig, 313 페이지	URL 필터링을 위한 고급 설정 구성	C Series, X Series, M Series
websecurityconfig, 315 페이지	URL 필터링을 위한 전역 설정 구성	C Series, X Series, M Series



2 장

명령행 인터페이스: 기초

이 장에는 다음 섹션이 포함되어 있습니다.

- CLI(Command Line Interface)에 액세스, 13 페이지
- 명령줄 인터페이스 규칙, 14 페이지
- 범용 CLI 명령, 17 페이지
- 배치 명령, 19 페이지

CLI(Command Line Interface)에 액세스

명령줄 인터페이스는 IP 인터페이스의 SSH 또는 텔넷을 통해(해당 서비스가 활성화된 경우) 액세스하거나 시리얼 포트에서 터미널 에뮬레이션 소프트웨어를 통해 액세스할 수 있습니다. 기본적으로 SSH 및 텔넷은 관리 포트에서 구성합니다. `interfaceconfig` 명령을 사용하여 이러한 서비스를 비활성화할 수 있습니다.

CLI 액세스는 어플라이언스 설정 과정에서 선택된 관리 연결 방법에 따라 달라집니다. 공장 기본 사용자 이름 및 암호가 다음에 나열됩니다. 처음에는 관리자 사용자 계정만 CLI에 액세스할 수 있습니다. 관리자 계정을 통해 커맨드 라인 인터페이스에 처음 액세스한 후에는 서로 다른 권한 레벨의 사용자를 추가할 수 있습니다. 시스템 설정 마법사에서 관리자 어카운트의 암호를 변경하라는 메시지를 표시합니다. 관리자 어카운트의 암호는 `password` 명령을 사용하여 언제든지 직접 재설정할 수도 있습니다.

이더넷을 통해 연결하려면 공장 기본 IP 주소인 192.168.42.42를 사용하여 SSH 또는 텔넷 세션을 시작합니다. SSH는 포트 22를 사용하도록 구성되었습니다. 텔넷은 포트 23을 사용하도록 구성되었습니다. 아래의 사용자 이름 및 암호를 입력합니다.

직렬 연결을 통해 연결하려면: 직렬 케이블이 연결된 PC의 통신 포트에서 터미널 세션을 시작합니다. 자세한 내용은 “설정 및 설치”장을 참조하십시오. 아래의 사용자 이름 및 암호를 입력합니다.

아래의 사용자 이름 및 암호를 입력하여 어플라이언스에 로그인합니다.

공장 기본 사용자 이름 및 암호

- 사용자 이름: **admin**
- 암호: **ironport**

예를 들면 다음과 같습니다.

```
login: admin
```

```
passphrase: ironport
```

명령줄 인터페이스 규칙

이 섹션에서는 AsyncOS CLI 규칙에 대해 설명합니다.

명령 프롬프트

최상위 명령 프롬프트는 정규화된 호스트 이름, > 기호, 공백 순으로 구성됩니다. 예를 들면 다음과 같습니다.

```
mail3.example.com>
```

어플라이언스가 중앙 집중식 관리 기능을 사용하여 클러스터의 일부로 구성된 경우 CLI 프롬프트는 현재 모드를 나타내도록 변경됩니다. 예를 들면 다음과 같습니다.

```
(Cluster Americas) >
```

또는

```
(Machine los_angeles.example.com)
>
```

자세한 내용은 사용 설명서에서 “중앙 집중식 관리”를 참조하십시오.

명령을 실행할 때 CLI에서 사용자의 입력이 필요합니다. CLI에서 사용자 입력을 요청할 때 명령 프롬프트에는 대괄호([])와 > 기호로 구성된 기본 입력이 표시됩니다. 기본 입력이 없을 경우 명령 프롬프트 괄호는 비어 있습니다.

예를 들면 다음과 같습니다.

```
Please create a fully-qualified hostname for this Gateway
(Ex: "mail3.example.com"):
[]>
mail3.example.com
```

기본 설정이 있으면 그 설정이 명령 프롬프트 괄호 안에 표시됩니다. 예를 들면 다음과 같습니다.

```
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[1]> 1
```

기본 설정이 표시된 경우 Return을 입력하는 것은 기본값을 입력하는 것과 동일합니다.

```
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[1]> (type Return)
```

명령 구문

인터랙티브 모드에서 동작하는 경우 CLI 명령 구문은 공백과 인수 또는 매개변수 없이 단일 명령으로 구성됩니다. 예를 들면 다음과 같습니다.

```
mail3.example.com> systemsetup
```

선택 목록

입력에 대해 여러 선택 항목이 제공될 경우 숫자가 지정된 목록을 사용하는 명령도 있습니다. 프롬프트에 선택할 번호를 입력합니다.

예를 들면 다음과 같습니다.

```
Log level:
1. Error
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

예/아니요 쿼리

Yes 또는 No 옵션이 제공되는 경우 질문과 함께 기본값이 괄호 안에 표시됩니다. Y, N 또는 Yes, No로 답할 수 있습니다. 대소문자는 구분하지 않습니다.

예를 들면 다음과 같습니다.

```
Do you want to enable FTP on this interface? [Y]>
n
```

하위 명령

일부 명령에는 하위 명령이 있습니다. 하위 명령에는 NEW, EDIT 및 DELETE와 같은 지시문이 포함됩니다. EDIT 및 DELETE의 경우 이전에 시스템에 구성한 레코드 목록을 제공합니다.

예를 들면 다음과 같습니다.

```
mail3.example.com> interfaceconfig
Currently configured interfaces:
1. Management (192.168.42.42/24: mail3.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[ ]>
```

하위 명령에서 빈 프롬프트에 Enter 또는 Return을 입력하면 기본 명령으로 돌아갑니다.

Esc

하위 명령에서 언제든지 Ctrl-C 키보드 바로 가기를 사용하여 해당 명령을 종료한 후 즉시 CLI의 최상위 레벨로 돌아갈 수 있습니다.

기록

CLI는 세션 중에 입력한 모든 명령의 기록을 보관합니다. 키보드의 위쪽 및 아래쪽 화살표 키를 사용하거나 Ctrl-P 및 Ctrl-N 키 조합을 사용하여 실행되고 있는 최근에 사용한 명령의 목록을 스크롤할 수 있습니다.

```
mail3.example.com> (type the Up arrow key)
```

```
mail3.example.com> interfaceconfig (type the Up arrow key)
```

```
mail3.example.com> topin (type the Down arrow key)
```

명령 완성

명령줄 인터페이스에서는 명령 완성을 지원합니다. 일부 명령의 처음 몇 글자를 입력하고 Tab 키를 누르면 CLI가 고유 명령에 해당하는 문자열을 완성합니다. 입력하는 글자가 명령과 일치하지 않는 경우, CLI는 범위를 “줄입니다”. 예를 들면 다음과 같습니다.

```
mail3.example.com> set (type the Tab key)
setgateway, sethostname, setttime, settz
mail3.example.com> seth
(typing the Tab again completes the entry with sethostname)
```

CLI의 기록 및 파일 완성 기능을 확인하려면 Enter 또는 Return을 입력하여 해당 명령을 호출해야 합니다.

컨피그레이션 변경

이메일 운영이 정상적으로 진행되는 동안에는 컨피그레이션을 변경할 수 있습니다.

컨피그레이션 변경은 다음 단계를 완료해야 적용됩니다.

프로시저

-
- 단계 1 명령 프롬프트에서 `commit` 명령을 실행합니다.
 - 단계 2 `commit` 명령에 필요한 명령을 입력합니다.
 - 단계 3 CLI에서 `commit` 절차에 대한 확인을 수신합니다.
-

다음에 수행할 작업

커밋되지 않은 구성 변경사항은 기록되지만, `commit` 명령을 실행할 때까지 적용되지 않습니다.



참고 어떤 명령에서는 `commit` 명령의 실행이 필요하지 않습니다. 커밋이 실행되어야 변경이 적용되는 명령에 대한 요약은 [CLI 빠른 참조 설명서, 1 페이지](#)를 참조하십시오.

CLI 세션을 종료하거나 시스템을 종료하거나 재부팅하거나 오류가 발생하거나 `clear` 명령을 실행하면 아직 커밋되지 않은 변경이 사라집니다.

범용 CLI 명령

이 섹션에서는 변경사항 커밋 및 지우기, 도움말 찾기, 명령줄 인터페이스 종료에 사용하는 명령에 대해 설명합니다.

컨피그레이션 변경 커밋

`commit` 명령은 어플라이언스의 구성 변경사항을 저장하는 필수 명령입니다. 구성 변경사항의 대부분이 `commit` 명령을 입력할 때까지 적용되지 않습니다. (일부 명령의 경우 변경사항을 적용하기 위해 `commit` 명령을 사용하지 않아도 됩니다.) `commit` 명령은 마지막 `commit` 명령 또는 마지막 `clear` 명령이 실행된 이후의 컨피그레이션 변경 사항에 적용됩니다. 최대 255자의 주석을 포함할 수 있습니다. 타임스탬프로 확인을 받을 때까지 변경사항은 커밋되지 않습니다.

`commit` 명령 다음에 주석을 입력하는 것은 선택 사항입니다.

```
mail3.example.com> commit
Please enter some comments describing your changes:
[ ]> Changed "psinet" IP Interface to a different IP address
Do you want to save the current configuration for rollback? [Y]>
n
Changes committed: Fri May 23 11:42:12 2014 GMT
```



참고 변경사항을 성공적으로 커밋하려면 최상위 명령 프롬프트에서 수행해야 합니다. 빈 프롬프트에 Return 을 입력하면 명령줄 계층에서 한 수준 위로 이동합니다.

컨피그레이션 변경 지우기

`clear` 명령은 마지막 `commit` 또는 `clear` 명령이 실행된 이후의 모든 컨피그레이션 변경 사항을 지웁니다.

```
mail3.example.com> clear
Are you sure you want to clear all changes since the last commit? [Y]>
y
Changes cleared: Mon Jan 01 12:00:01 2003
mail3.example.com>
```

명령줄 인터페이스 세션 종료

`quit` 명령을 사용하면 CLI 애플리케이션에서 로그아웃됩니다. 커밋되지 않은 구성 변경사항은 지워집니다. 이메일 작업에는 `quit` 명령이 적용되지 않습니다. 로그아웃 정보는 로그 파일에 기록됩니다. (`exit` 명령은 `quit` 명령과 동일합니다.)

```
mail3.example.com> quit
Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.
Are you sure you wish to exit? [N]> y
```

명령줄 인터페이스에서 도움말 찾기

`help` 명령은 사용 가능한 모든 CLI 명령을 나열하고 각 명령에 대한 간략한 설명을 제공합니다. `help` 명령은 명령 프롬프트에 `help` 또는 단일 물음표(?)를 입력하여 호출할 수 있습니다.

```
mail3.example.com> help
```

배치 명령

AsyncOS에서는 특정 CLI 명령을 새로운 단일행 CLI 형식으로 실행할 수 있도록 배치 명령 형식도 지원됩니다. 이 형식을 사용하면 작업을 완수하는 데 필요한 입력의 수가 줄어들고 공통적인 컨피그레이션 작업을 손쉽게 자동화하는 메커니즘이 제공됩니다. 또한 배치 명령을 사용하면 원격에서 SSH 클라이언트를 사용하여 명령을 실행할 수 있습니다. 그러면 손쉽게 CLI 명령을 스크립팅하고 여러 어플라이언스에서 한꺼번에 실행할 수 있습니다.

모든 명령에 배치 버전이 있는 것은 아니지만, 모든 배치 명령은 비 배치 명령으로 실행 가능합니다.

배치 명령 구문은 사용 중인 명령에 따라 달라집니다. 명령별 구문에 대한 자세한 내용은 [명령: 참조 예제, 23 페이지](#)의 CLI 예를 참조하십시오.

배치 명령의 예

다음 예에서는 발신자 그룹 REDLIST가 생성됩니다. 그런 다음 정책 THROTTLED와 연결되고 발신자 'possible_spammer.com'이 발신자 그룹에 추가됩니다.

CLI에서 이 작업을 실행하려면

```
example.com> listenerconfig
```

```
Currently configured listeners:
```

1. IncomingMail (on Management, 192.168.42.42/24) SMTP TCP Port 25 Public
2. OutgoingMail (on Data 2, 192.168.40.42/24) SMTP TCP Port 25 Private

```
Choose the operation you want to perform:
```

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

```
[ ]> edit
```

```
Enter the name or number of the listener you wish to edit.
```

```
[ ]> IncomingMail
```

```
Choose the operation you want to perform:
```

- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.

```
[ ]> HOSTACCESS
```

```
There are currently 4 policies defined.
```

```
There are currently 5 sender groups.
```

```
Choose the operation you want to perform:
```

```

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.

[ ]> NEW

1. New Sender Group
2. New Policy

[1]> 1

Enter a name for this sender group. (optional)

[ ]> REDLIST

Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed.
IP address ranges such as 10.1.1.10-20 are allowed. IP subnets such as
10.2.3. are allowed.

Hostnames such as crm.example.com are allowed.

Partial hostnames such as .example.com are allowed.

Ranges of SenderBase Reputation scores such as SBRs[7.5:10.0] are
allowed.

SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blacklist queries such as dnslist[query.blacklist.example] are
allowed.

Separate multiple hosts with commas

[ ]> possible_spammer.com

Select a behavior for this entry.

1. Accept
2. Relay
3. Reject
4. TCP Refuse
5. Continue
6. Policy: ACCEPTED
7. Policy: BLOCKED
8. Policy: THROTTLED
9. Policy: TRUSTED

[1]> 8

Enter a comment for this sender group.
[ ]>

There are currently 4 policies defined.
There are currently 6 sender groups.

```

CLI 배치 명령을 사용하여 동일한 작업을 수행하려면:


```
example.com> listenerconfig edit IncomingMail hostaccess new sendergroup  
REDLIST possible_spammer.com Policy: "THROTTLED"
```




3 장

명령: 참조 예제

이 장에는 다음 섹션이 포함되어 있습니다.

- [목록을 읽는 방법, 24 페이지](#)
- [AMP\(Advanced Malware Protection\), 24 페이지](#)
- [Anti-Spam, 34 페이지](#)
- [그рей메일 탐지 및 안전한 수신 거부, 40 페이지](#)
- [Anti-Virus, 42 페이지](#)
- [명령줄 관리, 45 페이지](#)
- [컨피그레이션 파일 관리, 48 페이지](#)
- [외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 52 페이지](#)
- [클러스터 관리, 56 페이지](#)
- [데이터 유출 방지, 58 페이지](#)
- [도메인 예외 목록, 59 페이지](#)
- [S/MIME 보안 서비스, 60 페이지](#)
- [도메인 키, 62 페이지](#)
- [DMARC 확인, 73 페이지](#)
- [DNS, 77 페이지](#)
- [How-Tos 위젯을 사용하여 사용자 경험 향상, 87 페이지](#)
- [일반 관리 및 문제 해결, 88 페이지](#)
- [콘텐츠 스캔, 146 페이지](#)
- [LDAP, 146 페이지](#)
- [메일 전달 컨피그레이션/모니터링, 153 페이지](#)
- [네트워크 컨피그레이션/네트워크 툴, 187 페이지](#)
- [신종 바이러스 필터\(Outbreak Filter\), 206 페이지](#)
- [정책 시행, 209 페이지](#)
- [로깅 및 알림, 246 페이지](#)
- [보고, 261 페이지](#)
- [Senderbase, 264 페이지](#)
- [발신자 도메인 평판 필터링, 265 페이지](#)
- [Smart Software Licensing, 269 페이지](#)

- SMTP 서비스 컨피그레이션, 273 페이지
- 시스템 설치, 307 페이지
- URL 필터링, 310 페이지
- 사용자 관리, 316 페이지
- 가상 어플라이언스 관리, 323 페이지
- 지리위치, 325 페이지

목록을 읽는 방법

각 명령에는 그에 대한 설명 및 하나 이상의 명령 사용 예제가 있습니다. 사용법 섹션에서는 다음 명령 특성을 지정합니다.

프로시저

단계 1 해당 명령이 어플라이언스에서 구현되려면 `commit` 명령이 필요한가?

단계 2 해당 명령은 특정 모드(클러스터, 그룹, 시스템)에 제한되는가?

단계 3 해당 명령은 배치 형식을 허용하는가?

중앙 집중식 관리에 대한 자세한 내용은 *AsyncOS for Cisco Email Security Appliances* 사용자 가이드를 참고하십시오.

배치 형식에 대한 자세한 내용은 [명령행 인터페이스: 기초, 13 페이지](#)를 참조하십시오.

AMP(Advanced Malware Protection)

- `ampconfig`, 24 페이지
- `ampstatus`, 33 페이지

ampconfig

파일 평판 필터링 및 파일 분석을 구성합니다. Cisco TAC의 지침 없이 고급 옵션을 수정하지 마십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help ampconfig` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

- 파일 평판 및 파일 분석 활성화, 25 페이지
- 파일 분석을 위한 파일 유형 선택, 26 페이지
- 퍼블릭 클라우드 파일 분석 서버를 사용하도록 ESA(Email Security Appliance) 구성, 27 페이지
- (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성, 28 페이지
- 온프레미스 파일 분석 서버를 사용하도록 ESA(Email Security Appliance) 구성, 29 페이지
- 온프레미스 파일 평판 서버를 사용하도록 ESA(Email Security Appliance) 구성, 30 페이지
- 로컬 파일 평판 캐시 지우기, 30 페이지
- 파일 평판 상태 값에 대한 캐시 만료 기간 구성, 31 페이지
- 파일 회귀 판정 알림 표시 안 함, 31 페이지
- 파일 분석을 위한 Cisco AMP Threat Grid 클러스터링 구성, 32 페이지

파일 평판 및 파일 분석 활성화

```
mail.example.com> amconfig
File Reputation: Disabled
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
[]> setup
File Reputation: Disabled
Would you like to use File Reputation? [Y]>
Would you like to use File Analysis? [Y]>
File types supported for File Analysis:
1. Microsoft Executables
Do you want to modify the file types selected for File Analysis? [N]>
Specify AMP processing timeout (in seconds)
[120]>
Advanced-Malware protection is now enabled on the system.
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy.
```

```

File Reputation: Enabled

File Analysis: Enabled

File types selected for File Analysis:

1. Microsoft Executables

Choose the operation you want to perform:

- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.

[]>

```

파일 분석을 위한 파일 유형 선택

```

mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> setup

File Reputation: Enabled
Would you like to use File Reputation? [Y]> yes

Would you like to use File Analysis? [Y]> yes

Do you want to modify the file types selected for File Analysis? [N]> yes

Enter comma separated serial numbers from the list of groups to select file types associated
with the group.

1. Archived and compressed
2. Configuration
3. Database
4. Document
5. Email
6. Encoded and Encrypted
7. Executables [partly selected]
8. Font & Graphics and Images
9. Microsoft Documents
10. Miscellaneous
11. Multimedia
[]> 9
File types belonging to the group "Microsoft Documents":
1. Access.Extension.14 (mda)
2. Access.MDBFile (mdb)
3. Access.MDEFile.14 (mde)
4. Access.Shortcut.DataAccessPage.1 (maw)
5. Access.Shortcut.Form.1 (maf)
6. ....

```

```

Choose the operation you want to perform:
- PRINT - Print the file types for File Analysis
- ADD - Add the file type(s) for File Analysis
[]> add
Choose the file type(s) to be added for File Analysis from the list
File types that are not selected for File Analysis from group "Microsoft Documents":
1. Access.Extension.14(mda)
2. Access.MDBFile(mdb)
3. Access.MDEFile.14(mde)
4. Access.Shortcut.DataAccessPage.1(maw)
5. Access.Shortcut.Form.1(maf)
6. .... ..
[]> 1-3, 5
Choose the operation you want to perform:
- PRINT - Print the file types for File Analysis
- DELETE - Delete the file type(s) for File Analysis
- ADD - Add the file type(s) for File Analysis
[]> print
File types belonging to the group:
1. Access.Extension.14(mda) [selected]
2. Access.MDBFile(mdb) [selected]
3. Access.MDEFile.14(mde) [selected]
4. Access.Shortcut.DataAccessPage.1(maw)
5. Access.Shortcut.Form.1(maf) [selected]
6. .... ..
Choose the operation you want to perform:
- PRINT - Print the file types for File Analysis
- DELETE - Delete the file type(s) for File Analysis
- ADD - Add the file type(s) for File Analysis
Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.

Please note: you must issue the 'policyconfig' command (CLI) or Mail Policies (GUI) to
configure advanced malware
scanning behavior for default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy. File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]>

```

퍼블릭 클라우드 파일 분석 서버를 사용하도록 ESA(Email Security Appliance) 구성

```

mail.example.com> amponfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.

```

```
[ ]> advanced
Enter cloud query timeout?
[15]>
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>
Enter cloud domain?
[cloud-domain.com]>
Do you want use the recommended analysis threshold from cloud service? [Y]>
Enter analysis threshold?
[50]>
Enter heartbeat interval?
[15]>
Do you want to enable SSL communication (port 443) for file reputation? [N]>
Do you want to suppress the verdict update alerts for all messages that are
not delivered to the recipient? [N]>
Choose a file analysis server:
1. AMERICAS (https://americas-fa.com)
2. Private Cloud
[1]>
...
```

(퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성

조직의 모든 콘텐츠 보안 어플라이언스에서 해당 조직의 모든 어플라이언스가 분석을 위해 보낸 파일에 대해 그 파일 분석 결과 세부 사항을 클라우드에서 보려면 모든 어플라이언스를 동일한 어플라이언스 그룹에 가입시켜야 합니다.

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

```
mail.example.com> amconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
  Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[ ]> setgroup
Does your organization have multiple Cisco Email, Web, and/or Content Security Management
appliances? [N]> Y
Do you want this appliance to display detailed analysis reports for files uploaded to the
cloud from other appliances in your organization,
and vice-versa?
[Y]> Enter an Analysis Group name. This name is case-sensitive and must be configured
identically on each appliance in the Analysis Group.
[ ]> FA_Reporting
Registration is successful with the group name. This does not require commit
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
  Microsoft Windows / DOS Executable
Appliance Group ID/Name: FA_Reporting
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- VIEWGROUP - view the group members details.
```



```
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```



참고 어플라이언스 그룹을 구성한 후에는 `setgroup` 하위 명령을 사용할 수 없습니다. 어떤 이유로든 그룹을 수정해야 하는 경우 Cisco TAC를 사용하여 케이스를 개설해야 합니다. `viewgroup` 하위 명령을 사용하여 어플라이언스 그룹의 상세정보를 볼 수 있습니다.

온프레미스 파일 분석 서버를 사용하도록 ESA(Email Security Appliance) 구성

```
mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced
Enter cloud query timeout?
[15]>
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>
Enter cloud domain?
[a.immunet.com]>
Do you want use the recommended analysis threshold from cloud service? [Y]>
Enter analysis threshold?
[50]>
Enter heartbeat interval?
[15]>
Do you want to enable SSL communication (port 443) for file reputation? [N]>
Do you want to suppress the verdict update alerts for all messages that are not delivered to the recipient? [N]>
Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]> 2
Enter file analysis server url?
[]> https://mycloud.example.com
Certificate Authority:
1. Use Cisco Trusted Root Certificate List
2. Paste certificate to CLI
[1]>
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

온프레미스 파일 평판 서버를 사용하도록 ESA(Email Security Appliance) 구성

```

mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[ ]> advanced
Enter cloud query timeout?
[15]>
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.domain.com)
2. Private reputation cloud
[1]> 2
Enter AMP reputation server hostname or IP address?
[ ]> myamp.domain.com
Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0
FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjDOL5UlsuusFncCzWBQ7RKNUSesmQRMSGkVb1/
3j+skZ6UtW+5u09lHNSj6tQ51s1SPrcBkedbNf0Tp0GbMJdyR4e9T04ZZwIDAQAB
-----END PUBLIC KEY-----
.
Enter cloud domain?
[immunet.com]>
Do you want use the recommended analysis threshold from cloud service? [Y]>
Enter heartbeat interval?
[15]>
Do you want to enable SSL communication (port 443) for file reputation? [N]>
Choose a file analysis server:
1. AMERICAS (https://threatgrid.com)
2. Private analysis cloud
[1]>
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[ ]>

```

로컬 파일 평판 캐시 지우기

```

mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:

```

```

- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> clearcache
Do you want to clear File Reputation Cache? [N]> y
Cache cleared successfully.
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>

```

파일 평판 상태 값에 대한 캐시 만료 기간 구성

다음 예에서는 `modifytimeout sub` 명령을 사용하여 악성 파일에 대한 캐시 만료 기간을 구성합니다.



참고 캐시 만료 기간은 15분에서 7일 사이의 값이어야 합니다.

```

mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> cachesettings
Choose the operation you want to perform:
- MODIFYTIMEOUT - Configure the cache expiry period based on File Reputation disposition.
- CLEARCACHE - Clears the local File Reputation cache.
[]> modifytimeout
Choose the operation you want to perform:
- CLEAN - Configure the cache expiry period for clean files.
- MALICIOUS - Configure the cache expiry period for malicious files.
- UNKNOWN - Configure the cache expiry period for unknown files.
[]> malicious
Specify the cache expiry period for this file disposition (use 'd' for days, 'h' for hours,
or 'm' for minutes). If you
specify a value without a unit, it is always treated as days.
[1d]> 5d

```

파일 회귀 판정 알림 표시 안 함

```

mail.example.com> ampconfig

File Reputation: Enabled

```

```

File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[>] advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.domain.com)
2. Private reputation cloud
[1]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]>

Do you want to suppress the file retrospective verdict alerts for the messages that are not
delivered to the recipient
[N]> yes

```

파일 분석을 위한 Cisco AMP Threat Grid 클러스터링 구성

```

mail.example.com> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[>] advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS (Legacy) (cloud-sa.amp.sourcefire.com)
3. Private reputation cloud
[1]>

Do you want use the recommended analysis threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]>

```

```
Do you want to suppress the verdict update alerts for all messages that are not
delivered to the recipient? [N]>
```

```
Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]> 2
```

```
There are no private analysis servers configured.
```

```
Choose the operation you want to perform:
- NEW - Configure a new private analysis server.
[ ]> new
```

```
Enter the file analysis server hostname or IP or URL.
[ ]> 192.1.10.20
```

```
Serial Number      Private Analysis Server
-----
1                  192.1.10.20
```

```
Choose the operation you want to perform:
- ADD - Add a new private analysis server to the cluster.
- EDIT - Edit a private analysis server in the cluster.
- DELETE - Delete a private analysis server from the cluster.
[ ]> add
```

```
Enter the new private analysis server hostname or IP address or URL to the
cluster.
[ ]> 192.1.10.30
```

```
Serial Number      Private Analysis Server
-----
1                  192.1.10.20
2                  192.1.10.30
```

```
Choose the operation you want to perform:
- ADD - Add a new private analysis server to the cluster.
- EDIT - Edit a private analysis server in the cluster.
- DELETE - Delete a private analysis server from the cluster.
[ ]>
```

ampstatus

설명

다양한 Advanced Malware Protection(파일 평판 및 분석) 구성 요소의 버전을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

예

```
mail.example.com> ampstatus
Component                               Version   Last Updated
AMP Client Settings                     1.0      Never updated
AMP Client Engine                       1.0      Never updated
```

Anti-Spam

이 섹션은 다음 명령으로 구성됩니다.

- [antispamconfig, 34 페이지](#)
- [antispamstatus, 35 페이지](#)
- [antispamupdate, 36 페이지](#)
- [incomingrelayconfig, 36 페이지](#)

antispamconfig

설명

안티스팸 정책을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 안티스팸 기능의 컨피그레이션을 보여줍니다.

```
mail3.example.com> antispamconfig
Choose the operation you want to perform:
- IRONPORT - Configure IronPort Anti-Spam.
- CLOUDMARK - Configure Cloudmark Service Provider Edition.
- MULTISCAN - Configure IronPort Intelligent Multi-Scan.
[ ]> ironport
IronPort Anti-Spam scanning: Disabled
Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[ ]> setup
IronPort Anti-Spam scanning: Disabled
Would you like to use IronPort Anti-Spam scanning? [Y]> y
The IronPort Anti-Spam License Agreement is displayed (if you have not already accepted it).
Do you accept the above IronPort Anti-Spam license agreement? [ ]> Y
Increasing the following size settings may result in decreased performance. Please consult documentation for size recommendations based on your environment.
```

```

Never scan message larger than: (Add a trailing K for kilobytes, M for megabytes, or no
letters for bytes.)
[1M]>
Always scan message smaller than: (Add a trailing K for kilobytes, M for megabytes, or no
letters for bytes.)
[512K]>
Please specify the IronPort Anti-Spam scanning timeout (in seconds)
[60]>
Would you like to enable regional scanning? [N]>
IronPort Anti-Spam scanning is now enabled on the system. Please note: you must issue the
'policyconfig' command (CLI)
or Mail Policies (GUI) to configure
Cisco IronPort scanning behavior for default and custom Incoming and Outgoing Mail Policies.
This is recommended for your DEFAULT policy.
IronPort Anti-Spam scanning: Enabled
Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[ ]>

```

antispamstatus

설명

안티스팸 상태를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> antispamstatus
Choose the operation you want to perform:
- IRONPORT - Display IronPort Anti-Spam version and rule information.
- CLOUDMARK - Display Cloudmark Service Provider Edition version and rule information.
- MULTISCAN - Display Intelligent Multi-Scan version and rule information.
[ ]> ironport
  Component                Last Update                Version
CASE Core Files            Never updated              3.4.0-013
CASE Utilities             Never updated              3.4.0-013
Structural Rules           Never updated 3.3.1-009-20141210_214201
Web Reputation DB          Never updated              20141211_111021
Web Reputation Rules       Never updated 20141211_111021-20141211_170330
Content Rules              Never updated              unavailable
Content Rules Update       Never updated              unavailable
Last download attempt made on: Never

```

antispamupdate

설명

안티스팸 규칙 및 관련 CASE 구성 요소를 즉시 업데이트하도록 수동으로 요청합니다. 여기에는 IMS(Intelligent Multi-Scan)에서 사용하는 안티스팸 규칙 및 CASE 구성 요소가 포함되지만 IMS에서 사용하는 서드파티 안티스팸 엔진은 해당되지 않습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> antispamupdate
Choose the operation you want to perform:
- MULTISCAN - Request updates for Intelligent Multi-Scan
- IRONPORT - Request updates for IronPort Anti-Spam
- CLOUDMARK - Request updates for Cloudmark Anti-Spam
[]> ironport
Requesting check for new CASE definitions
```

incomingrelayconfig

설명

수신 릴레이 기능을 활성화하고 구성할 때 **incomingrelayconfig** 명령을 사용합니다. 다음 예에서는 수신 릴레이 기능이 먼저 활성화된 다음 2개의 릴레이가 추가됩니다. 그중 하나는 수정되고 다른 하나는 삭제됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예: 수신 릴레이 활성화 수신 릴레이 구성

```
mail3.example.com> incomingrelayconfig
Incoming relays: Disabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- RELAYLIST - Configure incoming relays.
[]> setup
```



```

This command helps your Cisco IronPort appliance determine the sender's
originating IP address.
You should ONLY enable this command if your Cisco IronPort appliance is NOT
directly connected to the Internet as the "first hop" in your email
infrastructure.
You should configure this feature if other MTAs or servers are configured at
your network's perimeter to relay mail to your Cisco IronPort appliance.
Do you want to enable and define incoming relays? [N]> y
Incoming relays: Enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- RELAYLIST - Configure incoming relays.
[ ]> relaylist
There are no relays defined.
Choose the operation you want to perform:
- NEW - Create a new entry
[ ]> new
Enter a name for this incoming relay (Ex: "first-hop")
[ ]> first-hop
Enter the IP address of the incoming relay. IPv4 and IPv6 addresses are supported.
For IPv4, CIDR format subnets such as 10.1.1.0/24, IP address ranges such as 10.1.1.10-20,
and subnets such as 10.2.3. are allowed.
For IPv6, CIDR format subnets such as 2001:db8::/32 and IP address ranges such as
2001:db8::1-2001:db8::11 are allowed.
Hostnames such as crm.example.com and partial hostnames such as .example.com are allowed.
[ ]> 192.168.1.1
Do you want to use the "Received:" header or a custom header to determine the originating
IP address?
1. Use "Received:" header
2. Use a custom header
[1]> 1
Within the "Received:" header, enter the special character or string after which to begin
parsing for the originating IP address:
[from]> [
Within the headers, enter the position of the "Received:" header that contains the originating
IP address:
[1]> 1
There is 1 relay defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[ ]> print
Incoming
relay name:      IP address:      Header           Match           Hops:
-----
first-hop       192.168.1.1      Received         [               1
There is 1 relay defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[ ]> new
Enter a name for this incoming relay (Ex: "first-hop")
[ ]> second-hop
Enter the IP address of the incoming relay. IPv4 and IPv6 addresses are supported.
For IPv4, CIDR format subnets such as 10.1.1.0/24, IP address ranges such as 10.1.1.10-20,
and subnets such as 10.2.3. are allowed.
For IPv6, CIDR format subnets such as 2001:db8::/32 and IP address ranges such as
2001:db8::1-2001:db8::11 are allowed.
Hostnames such as crm.example.com and partial hostnames such as .example.com are allowed.
[ ]> 192.168.1.2

```

```

Do you want to use the "Received:" header or a custom header to determine the originating
IP address?
1. Use "Received:" header
2. Use a custom header
[1]> 2
Enter the custom header name that contains the originating IP address:
[1]> x-Connecting-IP
There are 2 relays defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[1]> print
Incoming
relay name:      IP address:      Header           Match           Hops:
-----
first-hop       192.168.1.1      Received         [               1
second-hop      192.168.1.2      x-Connecting-IP n/a             n/a
There are 2 relays defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[1]> delete
1. first-hop:      192.168.1.1
2. second-hop:    192.168.1.2
Enter the number of the entry you wish to delete:
[1]> 1
Incoming relay "first-hop" deleted.
There is 1 relay defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[1]>

```

sblconfig

설명

엔드 유저 허용 목록/차단 목록을 구성합니다.



참고 이 명령을 실행하려면 어플라이언스에서 GUI를 통해 허용 목록/차단 목록이 활성화되어야 합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식 - 가져오기

Batch Format

엔드 유저 허용 목록/차단 목록의 모든 항목을 지정된 파일의 항목으로 대체합니다.

```
slblconfig import <filename> <ignore invalid entries>
```

- filename - 가져올 파일의 이름. 이 파일은 어플라이언스의 /configuration 디렉터리에 있어야 합니다.
- ignore invalid entries - 잘못된 항목을 무시할지 여부. 'Yes' 또는 'No'입니다.

배치 형식 - 내보내기

엔드 유저 허용 목록/차단 목록의 모든 항목을 어플라이언스의 파일에 내보냅니다.

```
slblconfig export
```

어플라이언스에서는 다음 명령 규칙을 사용하여 .CSV 파일을 /configuration 디렉터리에 저장합니다.

slbl<timestamp><serial number>.csv.

예 - 허용 목록/차단 목록 항목 가져오기

```
mail.example.com>
slblconfig
End-User Safelist/Blocklist: Enabled
Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[]>
import
Currently available End-User Safelist/Blocklist files:
1. slbl.csv
Choose the file to import from.
[1]>
1
Do you want to ignore invalid entries? [Y]>
Y
End-User Safelist/Blocklist import has been initiated...
Please wait while this operation executes.
End-User Safelist/Blocklist successfully imported.
Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[]>
```

그레이메일 탐지 및 안전한 수신 거부

작업	명령
그레이메일 탐지 및 안전 수신 거부의 전역 설정 구성	graymailconfig, 40 페이지
그레이메일 탐지 및 안전 수신 거부를 위해 수신 메일 정책 구성	policyconfig, 216 페이지
기존 그레이메일 규칙의 세부 사항 표시	graymailstatus, 41 페이지
그레이메일 규칙의 업데이트 수동 요청	graymailupdate, 41 페이지

graymailconfig

설명

그레이메일 탐지 및 안전 수신 거부의 전역 설정을 구성합니다.



참고 그레이메일 탐지 및 안전 수신 거부를 활성화하려면 안티스팸 검사가 전역 범위에서 활성화되어야 합니다. 이는 IronPort Anti-Spam 또는 Intelligent Multi-Scan 기능으로 가능합니다.

그레이메일 탐지 및 안전 수신 거부의 정책 설정을 구성하려면 `policyconfig` 명령을 사용합니다. 자세한 내용은 [벌크 이메일 또는 소셜 네트워크 이메일로 식별된 메시지를 삭제하는 수신 정책 생성, 234 페이지](#)를 참고하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help graymailconfig` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

```
Graymail Detection: Disabled
```

```
Choose the operation you want to perform:
- SETUP - Configure Graymail.
[ ]> setup
```

```
Would you like to use Graymail Detection? [Y]>
```

```
Increasing the following size settings may result in decreased performance.
Please consult documentation for size recommendations based on your
environment.
```

```

Maximum Message Size to Scan (Add a trailing K for kilobytes, M for megabytes,
or no letters for bytes.):
[1M]>

Timeout for Scanning Single Message(in seconds):
[60]>

Would you like to enable automatic updates for Graymail engine? [Y]> Y

Graymail Safe Unsubscribe: Disabled

Would you like to use Graymail Safe Unsubscribe? [Y]>

Graymail Detection and Safe Unsubscribe is now enabled. Please note: The global
settings are recommended only for your DEFAULT mail policy. To configure policy
settings, use the incoming or outgoing policy page on web interface or the
'policyconfig' command in CLI.

```

graymailstatus

설명

기존 그레이메일 규칙의 세부 사항을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail.example.com> graymailstatus
Component          Version          Last Updated
Graymail Engine    01.378.53       Never Updated
Graymail Rules     01.378.53#15   Never updated
Graymail Tools     1.0.03         Never updated

```

graymailupdate

설명

그레이메일 규칙의 업데이트를 수동으로 요청합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> graymailupdate
Requesting check for new Graymail updates.
```

Anti-Virus

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [antivirusconfig, 42 페이지](#)
- [antivirusstatus, 44 페이지](#)
- [antivirusupdate, 44 페이지](#)

antivirusconfig

설명

안티바이러스 정책을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 `antivirusconfig` 명령을 사용하여 시스템에 대한 Sophos 바이러스 검사를 활성화하고 시간 초과 값을 60초로 설정합니다. 업데이트 서버, 업데이트 간격, 선택 사항인 프록시 서버를 구성하려면 [updateconfig, 139 페이지](#)를 참조하십시오.



참고

`systemsetup` 명령에서 라이선스에 동의하지 않은 경우 `antivirusconfig` 명령을 처음 실행할 때 라이선스 계약이 나타날 수 있습니다. 라이선스 계약에 동의하지 않으면 Sophos 바이러스 검사 엔진이 어플라이언스에서 활성화되지 않습니다.

```
mail3.example.com> antivirusconfig

Choose the operation you want to perform:
- SOPHOS - Configure Sophos Anti-Virus.
- MCAFEE - Configure McAfee Anti-Virus.
[]> sophos

Sophos Anti-Virus: Disabled

Choose the operation you want to perform:
```

```

- SETUP - Configure Sophos Anti-Virus.

[]> setup

Sophos Anti-Virus scanning: Disabled

Would you like to use Sophos Anti-Virus scanning? [Y]> y

(First time users see the license agreement displayed here.)

Please specify the Anti-Virus scanning timeout (in seconds)
[60]> 60

Would you like to enable automatic updates for Sophos engine? [Y] > Y

Sophos Anti-Virus scanning is now enabled on the system.

Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure Sophos Anti-Virus scanning behavior for default and custom
Incoming and Outgoing Mail Policies.
This is recommended for your DEFAULT policy.

Sophos Anti-Virus: Enabled
Choose the operation you want to perform:

- SETUP - Configure Sophos Anti-Virus.
[]>

```

안티바이러스 IDE 세부 사항 보기

AsyncOS에서는 어플라이언스에서 다운로드한 특정 안티바이러스 시그니처 파일(IDE 파일)의 상태 세부 사항을 제공합니다. **antivirusconfig -> detail** 하위 명령을 사용하여 이러한 상세정보에 액세스할 수 있습니다. 예를 들면 다음과 같습니다.

```

mail3.example.com> antivirusconfig
Choose the operation you want to perform:
- SOPHOS - Configure Sophos Anti-Virus.
- MCAFEE - Configure McAfee Anti-Virus.
[]> sophos
Sophos Anti-Virus: Enabled
Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
- STATUS - View Sophos Anti-Virus status.
- DETAIL - View Sophos Anti-Virus detail.
[]> detail
Sophos Anti-Virus:
Product - 3.87
Engine - 2.25.0
Product Date - 01 Nov 2004
Sophos IDEs currently on the system:
'Mkar-E.Ide'           Virus Sig. - 23 Dec 2004 01:24:02
'Rbot-Sd.Ide'         Virus Sig. - 22 Dec 2004 19:10:06
'Santy-A.Ide'         Virus Sig. - 22 Dec 2004 06:16:32
'Bacbanan.Ide'        Virus Sig. - 21 Dec 2004 18:33:58
'Rbot-Sb.Ide'         Virus Sig. - 21 Dec 2004 14:50:46
'Rbotry.Ide'          Virus Sig. - 21 Dec 2004 06:13:40
'Sdbot-Si.Ide'        Virus Sig. - 20 Dec 2004 20:52:04
'Odbbob-A.Ide'        Virus Sig. - 19 Dec 2004 23:34:06
'Rbot-Rw.Ide'         Virus Sig. - 19 Dec 2004 00:50:34
'Wortd.Ide'           Virus Sig. - 18 Dec 2004 07:02:44

```

```
'Delf-Jb.Ide'          Virus Sig. - 17 Dec 2004 22:32:08
[...command continues...]
```

antivirusstatus

설명

안티바이러스 상태를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> antivirusstatus
Choose the operation you want to perform:
- MCAFEE - Display McAfee Anti-Virus version information
- SOPHOS - Display Sophos Anti-Virus version information
[]> sophos
  SAV Engine Version      3.85
  IDE Serial              2004101801
  Engine Update           Mon Sep 27 14:21:25 2004
  Last IDE Update        Mon Oct 18 02:56:48 2004
  Last Update Attempt    Mon Oct 18 11:11:44 2004
  Last Update Success    Mon Oct 18 02:56:47 2004
```

antivirusupdate

설명

바이러스 정의를 수동으로 업데이트합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> antivirusupdate
Choose the operation you want to perform:
- MCAFEE - Request updates for McAfee Anti-Virus
- SOPHOS - Request updates for Sophos Anti-Virus
```



```
[ ]> sophos
Requesting update of virus definitions
mail3.example.com>
```

명령줄 관리

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [commit, 45 페이지](#)
- [commitdetail, 45 페이지](#)
- [clearchanges 또는 clear, 46 페이지](#)
- [help 또는 h 또는 ?, 46 페이지](#)
- [rollbackconfig, 47 페이지](#)
- [quit 또는 q 또는 exit, 47 페이지](#)

commit

설명

변경 사항을 커밋합니다. **commit** 명령 다음에 주석을 입력하는 것은 선택 사항입니다.

Usage(사용)

Commit: 해당 없음

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> commit
Please enter some comments describing your changes:
[ ]> Changed "psinet" IP Interface to a different IP ad dress
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

commitdetail

설명

마지막 **commit**에 대한 세부 정보를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> commitdetail
Commit at Mon Apr 18 13:46:28 2005 PDT with comments: "Enabled loopback".
mail3.example.com>
```

clearchanges 또는 clear

설명

clear 명령은 마지막 commit 또는 clear 명령이 실행된 이후의 모든 구성 변경 사항을 지웁니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> clear
Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Mon Jan 01 12:00:01 2003
mail3.example.com>
```

help 또는 h 또는 ?

설명

help 명령은 사용 가능한 모든 CLI 명령을 나열하고 각 명령에 대한 간략한 설명을 제공합니다. **help** 명령은 명령 프롬프트에 **help** 또는 단일 물음표(?)를 입력하여 호출할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> help
Displays the list of all available commands.
```

rollbackconfig

rollbackconfig 명령을 사용하면 이전에 커밋한 10가지 컨피그레이션 중 하나로 롤백할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> rollbackconfig
Previous Commits:
  Committed On                User          Description
-----
1. Fri May 23 06:53:43 2014    admin         new user
2. Fri May 23 06:50:57 2014    admin         rollback
3. Fri May 23 05:47:26 2014    admin
4. Fri May 23 05:45:51 2014    admin         edit user
Enter the number of the config to revert to.
[]> 2
Are you sure you want to roll back the configuration? [N]> y
Reverted to Fri May 23 06:50:57 2014    admin         rollback
Do you want to commit this configuration now? [N]> y
Committed the changes successfully
```

quit 또는 q 또는 exit

설명

quit 명령은 사용자를 CLI 애플리케이션에서 로그아웃합니다. 커밋되지 않은 구성 변경사항은 지워집니다. 이메일 작업에는 **quit** 명령이 적용되지 않습니다. 로그아웃 정보는 로그 파일에 기록됩니다. (exit 명령은 quit 명령과 동일합니다.)

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> quit
Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.
Are you sure you wish to exit? [N]> Y
```

컨피그레이션 파일 관리

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [loadconfig, 48 페이지](#)
- [mailconfig, 49 페이지](#)
- [resetconfig, 50 페이지](#)
- [saveconfig, 51 페이지](#)
- [showconfig, 51 페이지](#)

loadconfig

설명

컨피그레이션 파일을 로드합니다.



참고

클러스터링된 시스템에 컨피그레이션을 로드하는 것은 GUI를 사용할 때만 지원됩니다. 자세한 내용은 *AsyncOS for Cisco Email Security Appliances* 사용자 가이드를 참고하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 로컬 위치에서 새로운 컨피그레이션 파일을 가져옵니다.

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 2
Enter the name of the file to import:
[1]> changed.config.xml
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
Please enter some comments describing your changes:
[1]> loaded new configuration file
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

이 예제에서는 새 구성 파일을 명령줄에 직접 붙여 넣습니다. (붙여 넣기 명령을 종료하려면 빈 행에 Control-D를 입력해야 합니다.) 그런 다음 시스템 설정 마법사를 사용하여 기본 호스트 이름, IP 주소, 기본 게이트웨이 정보를 변경합니다. 마지막으로 변경 사항을 커밋합니다.

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 1
Paste the configuration file now.
Press CTRL-D on a blank line when done.
[The configuration file is pasted until the end tag
</config>
. Control-D is entered on a separate line.]
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> systemsetup
[The system setup wizard is run.]
mail3.example.com> commit
Please enter some comments describing your changes:
[ ]> pasted new configuration file and changed default settings via
systemsetup
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

mailconfig

설명

구성을 테스트하려면 **mailconfig** 명령을 사용하여 **systemsetup** 명령으로 방금 생성한 시스템 구성 데이터가 포함된 테스트 이메일을 즉시 전송하면 됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> mailconfig
Please enter the email address to which you want to send the configuration file.
Separate multiple addresses with commas.
[ ]> user@example.com
Choose the passphrase option:
1. Mask passphrases (Files with masked passphrases cannot be loaded using loadconfig command)
2. Encrypt passphrases
3. Plain passphrases
[1]> 2
The configuration file has been sent to user@example.com.
```

시스템이 네트워크에서 메일을 보낼 수 있음을 확인하기 위해 액세스 권한이 있는 사서함에 컨피그 레이션을 보냅니다.



참고 더 우수한 보안을 위해 어플라이언스의 중요 데이터 암호화 기능이 `fipsconfig` 명령에서 활성화된 경우 `Plain passwords` 옵션을 사용할 수 없습니다.

resetconfig

설명

어플라이언스를 물리적으로 옮기는 경우 공장 기본 설정으로 시작하길 원할 수 있습니다. `resetconfig` 명령은 모든 구성 값을 공장 기본값으로 재설정합니다. 이 명령은 매우 파괴적이므로 장치를 운반하거나 마지막 수단으로 구성 문제를 해결할 때만 사용해야 합니다. `resetconfig` 명령을 실행하고 CLI에 다시 연결한 다음 `systemsetup` 명령을 실행하는 것이 좋습니다.



참고 `resetconfig` 명령은 어플라이언스가 오프라인 상태일 때만 작동합니다. `resetconfig` 명령이 완료되면 `systemsetup` 명령을 다시 실행하지 않더라도 어플라이언스는 자동으로 온라인 상태가 됩니다. `resetconfig` 명령을 실행하기 전에 메일 전달이 일시 중단된 경우 `resetconfig` 명령이 완료되면 다시 메일 전달을 시도합니다.



위험 `resetconfig` 명령을 실행하면 모든 네트워크 설정이 공장 기본값으로 돌아가므로 잠재적으로 CLI에서 분리되고 어플라이언스에 연결하는 데 사용한 서비스(FTP, Telnet, SSH, HTTP, HTTPS)가 비활성화되며 심지어 `userconfig` 명령을 사용하여 생성한 추가 사용자 계정이 제거됩니다. 직렬 인터페이스를 사용하거나 기본 관리자 계정을 통해 관리 포트에서 기본 설정을 사용하여 CLI에 다시 연결할 수 없는 경우 이 명령을 사용하지 마십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> suspend
Delay (seconds, minimum 30):
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com>
```

```

resetconfig
Are you sure you want to reset all configuration values? [N]> Y
All settings have been restored to the factory default.

```

saveconfig

설명

saveconfig 명령은 구성 파일을 고유한 파일 이름으로 configuration 디렉터리에 저장합니다.



참고 클러스터링한 환경일 경우 이 명령은 전체 클러스터 컨피그레이션을 저장합니다. 클러스터링 시스템에서 이 명령을 실행하려면 컨피그레이션 모드를 클러스터로 변경합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 구성 파일의 암호를 암호화하여 configuration 디렉터리에 저장합니다.

```

mail.example.com> saveconfig
Choose the passphrase option:
1. Mask passphrases (Files with masked passphrases cannot be loaded using loadconfig command)
2. Encrypt passphrases

[1]> 2
File written on machine "mail.example.com" to the location
"/configuration/C100V-4232116C4E14C70C4C7F-7898DA3BD955-20140319T050635.xml".
Configuration saved.

```



참고 더 우수한 보안을 위해 어플라이언스의 중요 데이터 암호화 기능이 fipsconfig 명령에서 활성화된 경우 Plain passwords 옵션을 사용할 수 없습니다.

showconfig

설명

showconfig 명령은 현재 구성을 화면에 출력합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 구성을 CLI에 표시하고 구성의 암호를 암호화합니다.

```
mail.example.com> showconfig
Choose the passphrase display option:
1. Mask passphrases (Files with masked passphrases cannot be loaded using loadconfig command)
2. Encrypt passphrases
3. Plain passphrases
[1]> 2
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: Cisco C100V Email Security Virtual Appliance
  Model Number: C100V
  Version: 9.0.0-038
  Serial Number: 4232116C4E14C70C4C7F-7898DA3BD955
  Number of CPUs: 2
  Memory (MB): 6144
  Current Time: Wed Mar 19 05:30:05 2014
-->
<config>
<!--
*****
*                               Network Configuration                               *
*****
-->[The remainder of the configuration file is printed to the screen.]
```



참고 더 우수한 보안을 위해 어플라이언스의 중요 데이터 암호화 기능이 fipsconfig 명령에서 활성화된 경우 Plain passwords 옵션을 사용할 수 없습니다.

외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이가 구성

- [threatfeedconfig](#), 53 페이지
- [threatfeedstatus](#), 54 페이지
- [threatfeedupdate](#), 55 페이지

threatfeedconfig

- 설명, 53 페이지
- Usage(사용), 53 페이지
- 예 - 외부 위협 피드 소스 추가, 53 페이지

설명

threatfeedconfig 명령은 다음에 사용됩니다.

- Cisco Email Security 게이트웨이에서 ETF 엔진을 활성화합니다.
- Cisco Email Security 게이트웨이에서 ETF 소스를 구성합니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예 - 외부 위협 피드 엔진 활성화

다음 예에서는 setup 하위 명령을 사용하여 Cisco Email Security 게이트웨이에서 ETF 엔진을 활성화할 수 있습니다.

```
mail.example.com> threatfeedconfig

Choose the operation you want to perform:
- SETUP - Configure External Threat Feeds.
- SOURCECONFIG - Configure an external threat feed source.

[]> setup
External Threat Feeds: Enabled
Would you like to use External Threat Feeds? [Y]> yes
Do you want to add a custom header to the message in the case of an External Threat Feeds
Lookup Failure? [N]> yes
Enter the header name:
[X-IronPort-ETF-Lookup-Failure]>

Enter the header content:
[true]>
Choose the operation you want to perform:
- SETUP - Configure External Threat Feeds.
- SOURCECONFIG - Configure an external threat feed source.

[]>
```

예 - 외부 위협 피드 소스 추가

다음 예에서는 sourceconfig 하위 명령을 사용하여 Cisco Email Security 게이트웨이에서 ETF 소스를 추가할 수 있습니다.

```

mail.example.com > threatfeedconfig
Choose the operation you want to perform:
- SOURCECONFIG - Configure an external threat feed source.
[]> sourceconfig
Choose the operation you want to perform:
- ADD - Add a Source.
- LIST - List out all the sources.
- DETAIL - Get detailed information about a source.
- EDIT - Edit a source.
- SUSPEND - Suspend a source.
- RESUME - Resume a source.
- DELETE - Delete a source.
[]> add
Choose the operation you want to perform:
- POLL URL - Add an external threat feed source using the polling path and collection name.
[]> poll url
Enter a name for the external threat feed source:
[]> test_source
Enter a description for the external threat feed source (optional):
[]> test_source
Enter the host name for the external threat feed source:
[]> hailataxii.com
Enter the polling path for the external threat feed source:
[]> /taxii-data
Enter the collection name for the external threat feed source:
[]> quest.Abuse_ch
Enter the polling interval:
The polling interval can be an alphanumeric value that consists of a combination of
minutes, hours, or days followed by 'm','h' or 'd' suffixes. The numeric
values that are not entered with a suffix are considered as minutes by default. The
minimum value is 15 minutes.
[60m]> 30

Enter the age of the threat feed:
The value for the age must be between 1 and 365 days. Enter the age of the threat feed
that you want to fetch from the TAXII server. For example, if the age
is 30 days, the appliance fetches all threat feeds whose age is up to 30 days only.
[30]> 20

Enter the time span for each poll segment:
The age of threat feeds for a poll can be split into different poll segments based
on the time span entered.
The minimum time span for a poll segment is 1 day. The maximum time span for a
poll segment is the value entered in the 'Age of Threat Feeds' field.
For example, if the age of the threat feeds is 30 days and the TAXII server has a fixed
limit on
the age of threat feeds (for example, '20 days'), enter the fixed limit, which must be less
than
the age of the threat feeds configured on your appliance.
[30]> 5

Do you want to use HTTPS? [Y]> yes
Enter the polling port:
[443]> 443
Do you want to use a proxy server for the threat feed source? [N]> no
Do you want to configure user credentials for the external threat feed source? [Y]> no
test_source successfully added.

```

threatfeedstatus

- [설명, 55 페이지](#)

- [Usage\(사용\), 55 페이지](#)
- [예 - 외부 위협 피드 엔진의 현재 버전 보기, 55 페이지](#)

설명

`threatfeedstatus` 명령은 ETF 엔진의 현재 버전을 표시하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예 - 외부 위협 피드 엔진의 현재 버전 보기

다음 예에서는 `threatfeedstatus` 명령을 사용하여 ETF 엔진의 현재 버전을 볼 수 있습니다.

```
mail.example.com> threatfeedstatus
Component          Version          Last Updated
External ThreatFeeds  1.0.0-0000001  2 Jul 2018 04:22 (GMT +00:00)
```

threatfeedupdate

- [설명, 55 페이지](#)
- [Usage\(사용\), 55 페이지](#)
- [예 - 외부 위협 피드 엔진 수동 업데이트, 55 페이지](#)

설명

`threatfeedupdate` 명령은 ETF 엔진을 수동으로 업데이트하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예 - 외부 위협 피드 엔진 수동 업데이트

다음 예에서는 `threatfeedupdate` 명령을 사용하여 ETF 엔진을 수동으로 업데이트할 수 있습니다.

```
mail.example.com > threatfeedupdate
Requesting check for new External Threat Feeds updates.
```

클러스터 관리

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [clusterconfig, 56 페이지](#)

clusterconfig

설명

clusterconfig 명령은 클러스터 관련 설정을 구성할 때 사용합니다. 해당 시스템이 클러스터에 포함되지 않은 경우 **clusterconfig**를 실행하면 클러스터에 가입하거나 새 클러스터를 생성하는 옵션이 나타납니다.

clusterconfig 명령은 추가 하위 명령을 제공합니다.

비 클러스터 명령

다음 명령은 클러스터에 포함되지 않은 경우에 사용할 수 있습니다.

- **clusterconfig new <name>** — 지정된 이름으로 새 클러스터를 생성합니다. 해당 시스템은 이 클러스터의 구성원이자 "Main Group"이라는 기본 클러스터 그룹의 구성원이 됩니다

<name> - 새 클러스터의 이름

- **clusterconfig join [--port=xx] <ip_of_remote_cluster> [<admin_password>]<groupname>** - 해당 시스템을 클러스터에 추가합니다.

여기서 각 항목은 다음을 나타냅니다.

<ip_of_remote_cluster> - 클러스터에 있는 다른 시스템의 IP 주소

<admin_password> - 클러스터의 관리자 비밀번호. CCS를 통해 가입하는 경우

지정해서는 안 됩니다.

<groupname> - 가입할 그룹의 이름

<port> - 연결할 원격 시스템의 포트(기본값은 22)

- **clusterconfig prepjoin print**

CCS 포트를 통해 해당 시스템을 클러스터에 가입시키기 위해 준비하는 데 필요한 정보를 표시합니다.

클러스터 명령

다음 명령은 클러스터에 있을 때 사용할 수 있습니다.

- **clusterconfig addgroup <groupname>** — 새 클러스터 그룹을 생성합니다. 이 그룹은 구성원이 없는 상태로 시작합니다.

- `clusterconfig renamegroup <old_groupname> <new_groupname>` — 클러스터 그룹의 이름을 변경합니다.
- `clusterconfig deletegroup <groupname> [new_groupname]` — 클러스터 그룹을 제거합니다.
 <groupname> - 제거할 클러스터 그룹의 이름
 <new_groupname> - 기존 그룹의 시스템을 옮길 클러스터 그룹
- `clusterconfig setgroup <machinename> <groupname>` — 해당 시스템이 속하는 그룹을 설정하거나 변경합니다.
 <machinename> - 설정할 시스템의 이름.
 <groupname> - 시스템을 설정할 그룹
- `clusterconfig removemachine <machinename>` — 클러스터에서 시스템을 제거합니다.
- `clusterconfig setname <name>` — 클러스터의 이름을 지정된 이름으로 변경합니다.
- `clusterconfig list` — 현재 클러스터에 있는 모든 시스템을 표시합니다.
- `clusterconfig connstatus` — 현재 클러스터에 있는 모든 시스템을 표시하고 연결이 끊긴 시스템의 라우팅 세부 사항을 추가합니다.
- `clusterconfig disconnect <machinename>` — 일시적으로 시스템을 클러스터에서 분리합니다.
 <machinename> - 연결을 끊을 시스템의 이름
- `clusterconfig reconnect <machinename>` - "disconnect" 명령으로 분리했던 시스템과의 연결을 복원합니다.
- `clusterconfig prepjoin new <serial_number> <hostname> <user_key>` — CCS 포트를 통해 클러스터에 가입할 새 호스트를 추가합니다.
 <serial_number> - 추가되는 시스템의 일련 번호
 <hostname> - 추가되는 시스템의 호스트 이름
 <user_key> - 가입한 시스템에서 실행한 "prepjoin print" 명령의 SSH 사용자 키.
- `clusterconfig prepjoin delete <serial_number|hostname>` — "prepjoin new" 명령에서 추가하도록 표시되었던 호스트를 제거합니다. 이는 나중에 그 호스트를 추가하지 않기로 결정한 경우에만 필요합니다. 호스트가 클러스터에 추가되면 그 prepjoin 정보가 자동으로 제거됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 클러스터 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

`clusterconfig` 명령 및 그 사용에 대한 설명은 *AsyncOS for Cisco Email Security Appliances* 사용자 가이드를 참고하십시오.

데이터 유출 방지

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [dlpstatus, 58 페이지](#)
- [dlpupdate, 58 페이지](#)

dlpstatus

DLP 엔진의 버전 정보를 요청합니다.



참고

dlpstatus 명령을 사용하려면 먼저 GUI의 DLP Global Settings(DLP 전역 설정) 페이지에서 DLP가 구성되어 있어야 합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 클러스터, 그룹 또는 시스템 모드에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> dlpstatus

Component          Version    Last Updated
DLP Engine         3.0.2.31  Never updated
```

dlpupdate

설명

DLP 엔진을 업데이트합니다.



참고

dlpupdate 명령을 사용하려면 먼저 GUI의 DLP Global Settings(DLP 전역 설정) 페이지에서 DLP가 구성되어 있어야 합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 클러스터, 그룹 또는 시스템 모드에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

dlpupdate 명령의 배치 형식은 변경 사항이 없더라도 DLP 엔진을 업데이트합니다.

```
dlpupdate [force]
```

예

```
mail.example.com> dlpupdate

Checking for available updates. This may take a few seconds..

Could not check for available updates. Please check your Network and Service Updates settings
and retry.

Choose the operation you want to perform:

- SETUP - Enable or disable automatic updates for DLP Engine.

[ ]> setup

Automatic updates for DLP are disabled

Do you wish to enable automatic updates for DLP Engine? [N]> y

Choose the operation you want to perform:

- SETUP - Enable or disable automatic updates for DLP Engine.

[ ]>
```

도메인 예외 목록

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [domainreconfig, 59 페이지](#)

domainreconfig

설명

domainreconfig 명령은 도메인 예외 목록을 생성하는 데 사용됩니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help domainreconfig` 명령을 입력하여 온라인 도움말을 참고하십시오.

예

다음 예에서는 `domainreconfig` 명령을 사용하여 도메인 예의 목록을 생성할 수 있습니다.

```
mail.example.com> domainreconfig

Would you like to configure an exception list for Sender Domain Reputation and
External Threat Feeds functionality? [N]> yes

Select the domain only address list to to be used for Sender Domain Reputation
and External Threat Feeds functionality

1. addr_list

[1]> 1
```

S/MIME 보안 서비스

smimeconfig

설명

프로필 전송, 공개 키 관리 등과 같은 S/MIME 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

- 서명 및 암호화를 위한 전송 프로필 생성, 60 페이지
- 암호화용 공개 키 추가, 61 페이지

서명 및 암호화를 위한 전송 프로필 생성

다음 예에서는 S/MIME를 사용하여 메시지를 서명하고 암호화하기 위한 전송 프로필을 생성하는 방법을 보여줍니다.

```
mail.example.com> smimeconfig
Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.
[ ]> gateway
Choose the operation you want to perform:
```



```

- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[ ]> sending
Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[ ]> new
Enter a name for this profile:
> hr_sign_and_encrypt
1. Encrypt
2. Sign
3. Sign/Encrypt
4. Triple
Enter S/MIME mode:
[2]> 3
1. smime_signing
Select S/MIME certificate to sign:
[1]>
1. Detached
2. Opaque
Enter S/MIME sign mode:
[1]>
1. Bounce
2. Drop
3. Split
Enter S/MIME action:
[1]> 3
Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[ ]> print
S/MIME Sending Profiles
Name          Certificate          S/MIME Mode    Sign Mode    Action
-----
hr_sign_a    smime_signing      Sign/Encrypt   Detached     Split
Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[ ]>

```

암호화용 공개 키 추가

다음 예에서는 메시지 암호화를 위해 수신자 S/MIME 인증서의 공개 키를 어플라이언스에 추가하는 방법을 보여줍니다.

```

mail.example.com> smimeconfig
Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.

```

```

[ ]> gateway
Choose the operation you want to perform:
- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[ ]> verification
Choose the operation you want to perform:
- NEW - Create a new S/MIME Public Key.
- IMPORT - Import the list of S/MIME Public Keys from a file.
[ ]> new
Enter a name for this profile:
> hr_signing
1. Import
2. Paste
Choose one of the options for the certificate introducing:
[2]>
Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDdDCCAlYgAwIBAgIBDTANBgkqhkiG9w0BAQUFADCBljELMAkGA1UEBhMCSU4x
CzAJBgNVBAG...
-----END CERTIFICATE-----
.
C=IN,ST=KA,L=BN,O=Cisco,OU=stg,CN=cert_for_enc,emailAddress=admin@example.com
Choose the operation you want to perform:
- NEW - Create a new S/MIME Public Key.
- EDIT - Edit a S/MIME Public Key.
- RENAME - Rename a S/MIME Public Key.
- DELETE - Delete a S/MIME Public Key.
- IMPORT - Import the list of S/MIME Public Keys from a file.
- EXPORT - Export the list of S/MIME Public Keys to a file.
- PRINT - Display S/MIME Public Keys.
[ ]> print
S/MIME Public Keys
Name          Emails          Domains          Remaining
-----
hr_signin    admin@vm30bsd0008.ibqa    dns.vm30bsd0008.ibqa    145 days

```

도메인 키

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [domainkeysconfig, 62 페이지](#)

domainkeysconfig

설명

DomainKeys/DKIM 지원을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.



참고 더 우수한 보안을 위해 어플라이언스의 중요 데이터 암호화 기능이 FIPS 모드에서 활성화된 경우 개인 키를 볼 수 없습니다. 개인 키를 수정하려는 경우 기존 개인 키를 입력하거나 새 개인 키를 생성할 수 있습니다.

배치 형식 - 서명 프로필

domainkeysconfig 명령의 배치 형식은 서명 프로필을 생성, 수정, 삭제할 때 사용할 수 있습니다.

- DomainKeys/DKIM 서명 프로필 추가:

```
domainkeysconfig profiles signing new <name> <type> <domain> <selector> <user-list>
[options]
```

표 1: domainkeysconfig 새 서명 프로필 인수

Argument	설명
<name>	도메인 프로필의 이름
<type>	도메인의 유형 dk 또는 dkim.
<domain>	도메인 프로필의 Domain 필드. Domain-Keys 서명의 d 태그를 형성합니다.
<selector>	도메인 프로필의 Selector 필드. Domain-Keys 서명의 s 태그를 형성합니다.
<user-list>	섬표로 구분된 도메인 프로필 사용자 목록. 사용자를 이메일 주소와 매치하여 특정 도메인 프로필을 이메일 서명에 사용할지 여부를 결정합니다. 모든 도메인 사용자를 매치하려면 특수 키워드 all을 사용합니다.
[옵션]	
--key_name	서명에 사용할 개인 키의 이름
--canon	DK 서명 시 사용할 정규화 알고리즘. 현재 지원되는 알고리즘은 simple 및 nofws입니다. 기본값은 nofws입니다.
--body_canon	DKIM 서명 시 사용할 본문 정규화 알고리즘. 현재 지원되는 알고리즘은 simple 및 relaxed입니다. 기본값은 simple입니다.
--header_canon	DKIM 서명 시 사용할 헤더 정규화 알고리즘. 현재 지원되는 알고리즘은 simple 및 relaxed입니다. 기본값은 simple입니다.
--body_length	서명 계산에 사용되는 정규화 본문의 바이트 수. DKIM 프로필에서만 사용합니다. 사용할 경우 이 값은 서명의 l 태그가 됩니다. 기본적으로 사용하지 않습니다.

Argument	설명
--headers_select	서명을 위해 헤더를 선택할 방법을 결정합니다. DKIM 프로필에서만 사용합니다. all, standard, standard_and_custom 중 하나입니다. all은 반복되지 않은 모든 헤더를 서명하는 것입니다. "standard"는 Subject, From, To, Sender, MIME 헤더 등 잘 알려진 헤더의 사전 정의 세트에 서명하는 것입니다. standard_and_custom은 잘 알려진 헤더 및 사용자 정의 헤더 세트에 서명하는 것입니다. 기본값은 standard입니다.
--custom_headers	서명할 사용자 정의 헤더 세트. headers_select가 standard_and_custom인 경우에만 DKIM 프로파일에서 사용됩니다. 기본값은 빈 세트입니다.
--i_tag	서명에 i 태그를 포함할지 여부를 결정합니다. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.
--agent_identity	이 메시지에 서명하는 사용자 또는 에이전트의 ID. 구문은 표준 이메일 주소이며, local-part는 생략할 수 있습니다. 이 주소의 domain 부분은 <domain>과 같거나 그 하위 도메인이어야 합니다. 이 옵션은 --i_tag 값이 yes로 설정된 경우에만 사용할 수 있습니다. 기본값은 빈 local-part 다음에 @, <domain>이 오는 것입니다.
--q_tag	서명에 q 태그를 포함할지 여부를 결정합니다. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.
--t_tag	서명에 t 태그를 포함할지 여부를 결정합니다. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.
--x_tag	서명에 x 태그를 포함할지 여부를 결정합니다. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.
--expiration_time	서명이 만료될 때까지의 시간(초).. DKIM 프로필에서만 사용합니다. 이 값은 서명의 x 태그와 t 태그의 차이가 됩니다. 이 옵션은 --x_tag 값이 yes로 설정된 경우에만 사용할 수 있습니다. 기본값은 31536000초(1년)입니다.
--z_tag	서명에 z 태그를 포함할지 여부를 결정합니다. 가능한 값은 yes 또는 no입니다. 기본값은 no입니다.

- 서명 프로필 수정:

```
domainkeysconfig profiles signing edit <name> [signing-profile-options]
```

서명 프로필 옵션:

- rename <name>
- domain <domain>
- selector <selector>
- canonicalization <canon>
- canonicalization <header_canon> <body_canon>
- key <key_name>

- bodylength <body_length>
- headersselect <header_select>
- customheaders <custom_headers>
- itag <i_tag> [<agent_identity>]
- qtag <q_tag>
- ttag <t_tag>
- xtag <x_tag> [<expiration_time>]
- ztag <z_tag>
- new <user-list>
- delete <user-list>
- print
- clear
- 서명 프로필 삭제:

```
domainkeysconfig profiles signing delete <name>
```

- 서명 프로필의 목록 표시:

```
domainkeysconfig profiles signing list
```

- 서명 프로필의 세부 사항 인쇄:

```
domainkeysconfig profiles signing print <name>
```

- 서명 프로필 테스트:

```
domainkeysconfig profiles signing test <name>
```

- 서명 프로필의 로컬 사본 가져오기:

```
domainkeysconfig profiles signing import <filename>
```

- 어플라이언스에서 서명 프로필의 복사본 내보내기:

```
domainkeysconfig profiles signing export <filename>
```

- 어플라이언스에서 모든 서명 프로필 삭제:

```
domainkeysconfig profiles signing clear
```

배치 형식 - 확인 프로필

- 새 DKIM 확인 프로필을 만듭니다.

```
domainkeysconfig profiles verification new <name> <verification-profile-options>
```

표 2: *domainkeysconfig* 확인 프로필 옵션

Argument	설명
--name	DKIM 확인 프로필의 이름
--min_key_size	허용 가능한 가장 작은 키. 가능한 키 길이 값(비트)은 512, 768, 1024, 1536, 2048입니다. 기본값은 512입니다.
--max_key_size	허용 가능한 가장 큰 키. 가능한 키 길이 값(비트)은 512, 768, 1024, 1536, 2048입니다. 기본값은 2048입니다.
--max_signatures_num	확인할 메시지의 최대 서명 수. 어떤 양수도 가능합니다. 기본값은 5입니다.
--key_query_timeout	키 쿼리가 시간 초과될 때까지의 시간(초). 어떤 양수도 가능합니다. 기본값은 10입니다.
--max_systemtime_divergence	발신인과 확인자 간의 벽시계 비동기 상태를 허용하는 시간(초). 어떤 양수도 가능합니다. 기본값은 60입니다.
--use_body_length	본문 길이 매개변수를 사용할지 여부. 가능한 값은 yes 또는 no입니다. 기본값은 yes입니다.
--tempfail_action	일시적 장애의 경우 이 SMTP 작업을 수행해야 합니다. 가능한 값은 accept 또는 reject입니다. 기본값은 accept입니다.
--tempfail_response_code	일시적 장애의 경우 거부된 메시지에 대한 SMTP 응답 코드. 4XX 형식의 숫자면 가능합니다. 기본값은 451입니다.
--tempfail_response_text	일시적 장애의 경우 거부된 메시지에 대한 SMTP 응답 텍스트. 기본값은 #4.7.5 Unable to verify signature - key server unavailable입니다.
--permfail_action	영구적 장애의 경우 이 SMTP 작업을 수행해야 합니다. 가능한 값은 accept 또는 reject입니다. 기본값은 accept입니다.
--permfail_response_code	영구적 장애의 경우 거부된 메시지에 대한 SMTP 응답 코드. 5XX 형식의 숫자면 가능합니다. 기본값은 550입니다.
--permfail_response_text	영구적 장애의 경우 거부된 메시지에 대한 SMTP 응답 텍스트. 기본값은 #5.7.5 DKIM unauthenticated mail is prohibited입니다.

- 확인 프로필 수정:

```
domainkeysconfig profiles verification edit <name> <verification-profile-options>
```

- 확인 프로필 삭제:

```
domainkeysconfig profiles verification delete <name>
```

- 기존 확인 프로필의 세부 사항 인쇄:

```
domainkeysconfig profiles verification print <name>
```

- 기존 확인 프로필의 목록 표시:

```
domainkeysconfig profiles verification list
```

- 로컬 시스템에서 확인 프로필 파일 가져오기:

```
domainkeysconfig profiles verification import <filename>
```

- 어플라이언스에서 확인 프로필 내보내기:

```
domainkeysconfig profiles verification export <filename>
```

- 어플라이언스에서 모든 확인 프로필 삭제:

```
domainkeysconfig profiles verification clear
```

배치 형식 - 서명 키

- 새 서명 키를 만듭니다.

```
domainkeysconfig keys new <key_name> <key-options>
```

표 3: *domainkeysconfig* 서명 키 옵션

Argument	설명
--generate_key	개인 키를 생성합니다. 가능한 키 길이 값(비트)은 512, 768, 1024, 1536, 2048입니다.
--use_key	제공된 개인 키를 사용합니다.
--public_key	지정된 개인 키에 대해 매치하는 공개 키를 가져와 화면에 인쇄하도록 플래그를 지정합니다. --generate_key가 먼저 지정될 경우 새 개인 키가 먼저 생성되고 매치하는 공개 키가 표시됩니다.

- 서명 키 수정:

```
domainkeysconfig keys edit <key_name> key <key-options>
```

- 기존 서명 키 이름 변경:

```
domainkeysconfig keys edit <key_name> rename <key_name>
```

- 공개 키 지정:

```
domainkeysconfig keys publickey <key_name>
```

- 키 삭제:

```
domainkeysconfig keys delete <key_name>
```

- 모든 서명 키 목록 표시:

```
domainkeysconfig keys list
```

- 지정된 서명 키에 대한 모든 정보 표시:

```
domainkeysconfig keys print <key_name>
```

- 로컬 시스템에서 서명 키 가져오기:

```
domainkeysconfig keys import <filename>
```

- 어플라이언스에서 서명 키 내보내기:

```
domainkeysconfig keys export <filename>
```

- 어플라이언스의 모든 서명 키 삭제:

```
domainkeysconfig keys clear
```

배치 형식 - 키 또는 프로필 검색

- 프로필 서명 키 검색:

```
domainkeysconfig search <search_text>
```


배치 형식 - 전역 설정

- 어플라이언스의 Domain Keys/DKIM 전역 설정을 수정합니다.

```
domainkeysconfig setup <setup_options>
```

사용 가능한 옵션:

- `--sign_generated_msgs` - 시스템에서 생성한 메시지를 서명할지 여부를 지정합니다. 가능한 값은 `yes` 또는 `no`입니다.

예: CLI에서 도메인 키 구성

어플라이언스의 도메인 키를 구성할 때 CLI에서 `domainkeysconfig` 명령을 사용합니다.

`domainkeysconfig` 명령은 **Mail Policies**(메일 정책) -> **Domain Keys**(도메인 키) 페이지의 모든 기능을 갖고 있습니다. 또한 샘플 Domain Keys DNS TXT 레코드를 생성할 수도 있습니다. 샘플 Domain Keys DNS TXT 레코드 생성에 대한 자세한 내용은 [샘플 Domain Keys DNS TXT 레코드 생성, 71 페이지](#)를 참고하십시오.

이 예에서는 키를 생성하고 도메인 프로필을 생성합니다.

```
mail3.example.com> domainkeysconfig
Number of DK/DKIM Signing Profiles: 0
Number of Signing Keys: 0
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> keys
No signing keys are defined.
Choose the operation you want to perform:
- NEW - Create a new signing key.
- IMPORT - Import signing keys from a file.
[]> new
Enter a name for this signing key:
[]> testkey
1. Generate a private key
2. Enter an existing key
[1]>
Enter the size (in bits) of this signing key:
1. 512
2. 768
3. 1024
4. 1536
5. 2048
[3]>
New key "testkey" created.
There are currently 1 signing keys defined.
Choose the operation you want to perform:
- NEW - Create a new signing key.
- EDIT - Modify a signing key.
- PUBLICKEY - Create a publickey from a signing key.
- DELETE - Delete a signing key.
```

```

- PRINT - Display signing keys.
- LIST - List signing keys.
- IMPORT - Import signing keys from a file.
- EXPORT - Export signing keys to a file.
- CLEAR - Clear all signing keys.
[]>
Number of DK/DKIM Signing Profiles: 0
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> profiles
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]> signing
No domain profiles are defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- IMPORT - Import domain profiles from a file.
[]> new
Enter a name for this domain profile:
[]> Example
Enter type of domain profile:
1. dk
2. dkim
[2]>
The domain field forms the basis of the public-key query. The value in
this field MUST match the domain of the sending email address or MUST
be one of the parent domains of the sending email address. This value
becomes the "d" tag of the Domain-Keys signature.
Enter the domain name of the signing domain:
[]> example.com
Selectors are arbitrary names below the "_domainkey." namespace. A
selector value and length MUST be legal in the DNS namespace and in
email headers with the additional provision that they cannot contain a
semicolon. This value becomes the "s" tag of the DomainKeys
Signature.
Enter selector:
[]> test
The private key which is to be used to sign messages must be entered.
A corresponding public key must be published in the DNS following the
form described in the DomainKeys documentation. If a key is not
immediately available, a key can be entered at a later time.
Select the key-association method:
1. Create new key
2. Paste in key
3. Enter key at later time
4. Select existing key
[1]> 4
Enter the name or number of a signing key.
1. testkey
[1]>
The canonicalization algorithm is the method by which the headers and
content are prepared for presentation to the signing algorithm.
Possible choices are "simple" and "relaxed".
Select canonicalization algorithm for body:
1. simple
2. relaxed
[1]> 1

```

```

How would you like to sign headers:
1. Sign all existing, non-repeatable headers (except Return-Path header).
2. Sign "well-known" headers (Date, Subject, From, To, Cc, Reply-To, Message-ID, Sender,
MIME headers).
3. Sign "well-known" headers plus a custom list of headers.
[2]>
Body length is a number of bytes of the message body to sign.
This value becomes the "l" tag of the signature.
Which body length option would you like to use?
1. Whole body implied. No further message modification is possible.
2. Whole body auto-determined. Appending content is possible.
3. Specify a body length.
[1]>
Would you like to fine-tune which tags should be used in the
DKIM Signature? (yes/no) [N]>
Finish by entering profile users. The following types of entries are
allowed:
- Email address entries such as "joe@example.com".
- Domain entries such as "example.com".
- Partial domain entries such as ".example.com". For example, a partial
domain of ".example.com" will match "sales.example.com". This
sort of entry will not match the root domain ("example.com").
- Leave blank to match all domain users.
Enter user for this signing profile:
[]> sales.example.com
Do you want to add another user? [N]>
There are currently 1 domain profiles defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]>
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]>
Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]>

```

샘플 Domain Keys DNS TXT 레코드 생성

```

mail3.example.com> domainkeysconfig
Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.

```

```

- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> profiles
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]> signing
There are currently 1 domain profiles defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]> dnstxt
Enter the name or number of a domain profile.
1. Example
[1]>
The answers to the following questions will be used to construct DKIM text
record for DNS. It can be used to publish information about this profile.
Do you wish to constrain the local part of the signing identities
("i=" tag of "DKIM-Signature" header field) associated with this
domain profile? [N]>
Do you wish to include notes that may be of interest to a human (no
interpretation is made by any program)? [N]>
The "testing mode" can be set to specify that this domain is testing DKIM and
that unverified email must not be treated differently from verified email.
Do you want to indicate the "testing mode"? [N]>
Do you wish to disable signing by subdomains of this domain? [N]>
The DKIM DNS TXT record is:
test._domainkey.example.com. IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDX5dOG9J8rXreA/uPtYr51rCTCqR+qlS5Gm
1f0QpLazSjE2BvQxZ5Nr+seOT+k7mDPOFSUHwCvO+kCum7fFRjS3E0F9jlpLdH5vz0CkP/wHdjPy3q6PSgJvtqvQ6v9E8k5U17C+DF6kVJUIJUSy5Ssu2
zmm9rKAH5m7FwIDAQAB;"
There are currently 1 domain profiles defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]>
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]>
Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.

```

```
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]>
```

DMARC 확인

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [dmarcconfig, 73 페이지](#)

dmarcconfig

설명

DMARC 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식 - DMARC 확인 프로필

dmarcconfig의 배치 형식은 확인 프로필을 생성, 수정, 삭제하고 전역 설정을 수정할 때 사용할 수 있습니다.

DMARC 확인 프로필 추가

```
dmarcconfig profiles new <name> [options]
```

Argument	설명
<name>	DMARC 프로필의 이름
[옵션]	
--rejectpolicy_action	DMARC 레코드의 정책이 reject일 때 AsyncOS에서 수행해야 할 메시지 작업. "reject", "quarantine" 또는 "none"입니다.
--rejectpolicy_response_code	거부된 메시지에 대한 SMTP 응답 코드. 기본값은 550입니다.
--rejectpolicy_response_text	거부된 메시지에 대한 SMTP 응답 텍스트. 기본값은 "#5.7.1 DMARC unauthenticated mail is prohibited."입니다.
--rejectpolicy_quarantine	DMARC 확인을 통과하지 못한 메시지의 격리

Argument	설명
--quarantinepolicy_action	DMARC 레코드의 정책이 quarantine일 때 AsyncOS에서 수행해야 할 메시지 작업 “quarantine” 또는 “none”입니다.
--quarantinepolicy_quarantine	DMARC 확인을 통과하지 못한 메시지의 격리
--tempfail_action	DMARC 확인 과정에서 일시적 장애가 발생하는 메시지에 대해 AsyncOS에서 수행해야 할 메시지 작업. “accept” 또는 “reject”입니다.
--tempfail_response_code	일시적 장애의 경우 거부된 메시지에 대한 SMTP 응답 코드. 기본값은 451입니다.
--tempfail_response_text	일시적 장애의 경우 거부된 메시지에 대한 SMTP 응답 텍스트. 기본값은 “#4.7.1 Unable to perform DMARC verification.”입니다.
--permfail_action	DMARC 확인 과정에서 영구적 장애가 발생하는 메시지에 대해 AsyncOS에서 수행해야 할 메시지 작업. “accept” 또는 “reject”입니다.
--permfail_response_code	영구적 장애의 경우 거부된 메시지에 대한 SMTP 응답 코드. 기본값은 550입니다.
--permfail_response_text	영구적 장애의 경우 거부된 메시지에 대한 SMTP 응답 텍스트. 기본값은 “#5.7.1 DMARC verification failed.”입니다.

DMARC 확인 프로파일 수정

```
dmarcconfig profiles edit <name> [options]
```

DMARC 확인 프로파일 삭제

```
dmarcconfig profiles delete <name>
```

모든 **DMARC** 확인 프로파일 삭제

```
dmarcconfig profiles clear
```

DMARC 확인 프로파일의 세부 사항 보기

```
dmarcconfig profiles print <name>
```

DMARC 확인 프로파일 내보내기

```
dmarcconfig profiles export <filename>
```

DMARC 확인 프로파일 가져오기

```
dmarcconfig profiles import <filename>
```

전역 설정 변경

dmarcconfig setup [options]

옵션	설명
--report_schedule	AsyncOS에서 DMARC 집계 보고서를 생성해야 하는 시간
--error_reports	DMARC 집계 보고서 크기가 10MB 또는 DMARC 레코드의 RUA 태그에 지정된 크기를 초과할 경우 도메인 소유자에게 전달 오류 보고서를 보냅니다.
--org_name	DMARC 집계 보고서를 생성하는 엔티티. 도메인 이름이어야 합니다.
--contact_info	DMARC 집계 보고서를 수신하는 도메인 소유자가 보고서를 생성한 엔티티와 연락하려는 경우 사용할 추가 연락처 정보(예: 조직의 고객 지원 정보).
--copy_reports	모든 DMARC 집계 보고서의 복사본을 특정 사용자(예: 집계 보고서에 대한 분석을 수행한 내부 사용자)에게 보냅니다. 하나의 이메일 주소 또는 쉼표로 구분된 여러 이메일 주소를 입력합니다.
--bypass_addresslist	특정 발신인(주소 목록)이 보낸 메시지는 DMARC 확인을 건너뜁니다. 참고 전체 이메일 주소로 생성된 주소 목록만 선택할 수 있습니다.
--bypass_headers	특정 헤더 필드 이름을 포함하는 메시지는 DMARC 확인을 건너뜁니다. 예를 들어 메일 목록 및 신뢰받는 전달자가 보낸 메시지에 대해 DMARC 검증을 건너뛰려면 이 옵션을 사용합니다. 하나의 헤더 또는 쉼표로 구분된 여러 헤더를 입력합니다.

예

다음 예에서는 DMARC 확인 프로필을 설정하고 DMARC 확인 프로필의 전역 설정을 수정하는 방법을 보여줍니다.

```
mail.example.com> dmarcconfig
Number of DMARC Verification Profiles: 1
Daily report generation time is: 00:00
Error reports enabled: No
Reports sent on behalf of:
Contact details for reports:
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: None Specified
Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[ ]> profiles
There are currently 1 DMARC verification profiles defined.
```

```

Choose the operation you want to perform:
- NEW - Create a new DMARC verification profile.
- EDIT - Modify a DMARC verification profile.
- DELETE - Delete a DMARC verification profile.
- PRINT - Display DMARC verification profiles.
- IMPORT - Import DMARC verification profiles from a file.
- EXPORT - Export DMARC verification profiles to a file.
- CLEAR - Clear all DMARC verification profiles.
[]> new
Enter the name of the new DMARC verification profile:
[]> dmarc_ver_profile_1
Select the message action when the policy in DMARC record is reject:
1. No Action
2. Quarantine the message
3. Reject the message
[3]> 1
Select the message action when the policy in DMARC record is quarantine:
1. No Action
2. Quarantine the message
[2]> 2
Select the quarantine for messages that fail DMARC verification (when the DMARC policy is quarantine).
1. Policy
[1]> 1
What SMTP action should be taken in case of temporary failure?
1. Accept
2. Reject
[1]> 2
Enter the SMTP response code for rejected messages in case of temporary failure.
[451]>
Enter the SMTP response text for rejected messages in case of temporary failure. Type DEFAULT
to use the default response text
'#4.7.1 Unable to perform
DMARC verification.'
[#4.7.1 Unable to perform DMARC verification.]>
What SMTP action should be taken in case of permanent failure?
1. Accept
2. Reject
[1]> 2
Enter the SMTP response code for rejected messages in case of permanent failure.
[550]>
Enter the SMTP response text for rejected messages in case of permanent failure. Type DEFAULT
to use the default response text
'#4.7.1 Unable to perform
DMARC verification.'
[#5.7.1 DMARC verification failed.]>
There are currently 2 DMARC verification profiles defined.
Choose the operation you want to perform:
- NEW - Create a new DMARC verification profile.
- EDIT - Modify a DMARC verification profile.
- DELETE - Delete a DMARC verification profile.
- PRINT - Display DMARC verification profiles.
- IMPORT - Import DMARC verification profiles from a file.
- EXPORT - Export DMARC verification profiles to a file.
- CLEAR - Clear all DMARC verification profiles.
[]>
Number of DMARC Verification Profiles: 2
Daily report generation time is: 00:00
Error reports enabled: No
Reports sent on behalf of:
Contact details for reports:
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: None Specified

```



```

Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]> setup
Would you like to modify DMARC report settings? (Yes/No) [N]> y
Enter the time of day to generate aggregate feedback reports. Use 24-hour format (HH:MM).
[00:00]>
Would you like to send DMARC error reports? (Yes/No) [N]> y
Enter the entity name responsible for report generation. This is added to the DMARC aggregate
reports.
[]> example.com
Enter additional contact information to be added to DMARC aggregate reports. This could be
an email address,
URL of a website with additional help, a phone number etc.
[]> http://dmarc.example.com
Would you like to send a copy of all aggregate reports? (Yes/No) [N]>
Would you like to bypass DMARC verification for an addresslist? (Yes/No) [N]>
Would you like to bypass DMARC verification for specific header fields? (Yes/No) [N]> y
Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
[]> add
Enter the header field name
[]> List-Unsubscribe
DMARC verification is configured to bypass DMARC verification for messages containing the
following header fields.
1. List-Unsubscribe
Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
- REMOVE - Remove a header field from the list.
[]> add
Enter the header field name
[]> List-ID
DMARC verification is configured to bypass DMARC verification for messages containing the
following header fields.
1. List-Unsubscribe
2. List-ID
Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
- REMOVE - Remove a header field from the list.
[]>
Number of DMARC Verification Profiles: 2
Daily report generation time is: 00:00
Error reports enabled: Yes
Reports sent on behalf of: example.com
Contact details for reports: http://dmarc.example.com
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: List-Unsubscribe, List-ID
Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]>

```

DNS

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [dig, 78 페이지](#)
- [dnsconfig, 80 페이지](#)
- [dnsflush, 84 페이지](#)

- [dnshostprefs, 84 페이지](#)
- [dnslistconfig, 85 페이지](#)
- [dnslisttest, 86 페이지](#)
- [dnsstatus, 86 페이지](#)

dig

설명

DNS 서버의 레코드를 조회합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

dig 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- DNS 서버의 레코드 조회

```
dig [options] [@<dns_ip>] [qtype] <hostname>
```

- DNS 서버에서 지정된 IP 주소에 대해 역방향 조회를 수행합니다.

```
dig -x <reverse_ip> [options] [@<dns_ip>]
```

dig 명령의 배치 형식에 사용할 수 있는 옵션입니다.

-s <source_ip>	Specify the source IP address.
-t	Make query over TCP.
-u	Make query over UDP (default).
dns_ip	Query the DNS server at this IP address.
qtype	Query type: A, PTR, CNAME, MX, SOA, NS, TXT.
hostname	Record that user want to look up.

```
reverse_ip - Reverse lookup IP address.
```

```
dns_ip - Query the DNS server at this IP address.
```

예

다음 예에서는 조회할 DNS 서버를 명시적으로 지정합니다.

```
mail.com> dig @111.111.111.111 example.com MX
; <<>> DiG 9.4.3-P2 <<>> @111.111.111.111 example.com MX
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18540
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; QUESTION SECTION:
example.com.                IN      MX
;; ANSWER SECTION:
mexample.com.              10800  IN      MX      10 mexample.com.
;; AUTHORITY SECTION:
example.com.              10800  IN      NS      test.example.com.
;; ADDITIONAL SECTION:
example.com. 10800 IN      A      111.111.111.111
example.com. 10800 IN      AAAA   2620:101:2004:4201::bd
example.com. 300   IN      A      111.111.111.111
;; Query time: 6 msec
;; SERVER: 10.92.144.4#53(10.92.144.4)
;; WHEN: Fri Dec 9 23:37:42 2011
;; MSG SIZE rcvd: 143
```



참고 **dig** 명령 사용 시 DNS 서버를 명시적으로 지정하지 않을 경우 이 명령은 Authority 및 Additional 섹션의 정보를 필터링합니다.

예: DNSSEC를 지원하는 DNS 서버의 TLSA 레코드 확인

다음 예에서는 TLSA 레코드를 명시적으로 확인합니다.

```
mail.example.com> dig

Enter the host or IP address to look up.
[ ]> example.com

Choose the query type:
1. A      the host's IP address
2. AAAA   the host's IPv6 address
3. CNAME  the canonical name for an alias
4. MX     the mail exchanger
5. NS     the name server for the named zone
6. PTR    the hostname if the query is an Internet address, otherwise the pointer to other
information
7. SOA    the domain's "start-of-authority" information
8. TLSA   TLSA Record
9. TXT    the text information
[1]> 8
```

```

Which interface do you want to query from?
1. Auto
2. Management
[1]> 2

Please enter the host or IP address of DNS server.
Leave the entry blank to use the default server.
Important! To perform DNSSEC queries, enter the host or IP address of the DNS Server supporting DNSSEC.
[]> 8.8.8.8

Do you want to make query over TCP? [N]>

Do you want to make a query over DNSSEC? [N]> Y

Please enter DNS key file path.
Leave the entry blank to use the default root keys
[]>

;; RRset to chase:
dane-esa.com.          3562      IN        MX        10 mx1.dane-esa.com.

;; RRSIG of the RRset to chase:
dane-esa.com.          3562      IN        RRSIG    MX 7 2 3600 20181028045140 20180928045140
43860 dane-esa.com.
K+t0W9aOqDMvxytXfkrms+IEUbK1Ct9XB5mBCCb3bHryvHs0cU6XPxTJ
XwQ5HUSWuQaC9MLyCA5Zn/AXlzbzKA7tGtnab0q3CmVKhhRXnIJ+jJht6
nuksUrLKsM6uYmR73DDM/bCC8n08w6nGeGq476mmNgETXAPfqSvHNuPp
DSquCG3nNfm8iE9XnG8jCKRPcKhWjROc/vmK6ZzuzFKCtT4QA/L5Ah0w
zffZqxR9Qmj3w8WQdz9eFAw5e0LFa5oR57i983ityJrQL4pjF17bwKNw
94xhqFlsWWKAC6wpoT64Doo00ou5TsKxHq5EwEat1OMIM0GHMniCuJcA K3seyQ==

```

dnsconfig

설명

DNS 설정 구성

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

dnsconfig 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 로컬 이름 서버 캐시를 사용하도록 DNS 구성:

```
dnsconfig parent new <ns_ip> <priority>
```

명령 인수:

- <ns_ip> - 이름 서버의 IP 주소. 여러 IP 주소를 쉼표로 구분합니다.
- <priority> - 이 항목의 우선 순위.
- 로컬 이름 서버 캐시 삭제:

```
dnsconfig parent delete <ns_ip>
```

- 특정 도메인에 사용할 대체 DNS 캐시 구성:

```
dnsconfig alt new <domains> <ns_ip>
```



참고 인터넷 루트 이름 서버가 쓰일 때는 사용할 수 없습니다.

명령 인수:

- <ns_ip> - 이름 서버의 IP 주소. 여러 IP 주소를 쉼표로 구분합니다.
- <domains> - 쉼표로 구분된 도메인 목록.
- 특정 도메인의 대체 DNS 캐시 삭제:

```
dnsconfig alt delete <domain>
```

- 인터넷 루트 이름 서버를 사용하도록 DNS 구성:

```
dnsconfig roots new <ns_domain> <ns_name> <ns_ip>
```

이름 서버 인수:

- <ns_domain> - 재정의할 도메인
- <ns_name> - 이름 서버의 이름
- <ns_ip> - 이름 서버의 IP 주소



참고 어떤 도메인에 대해 대체 이름 서버를 지정하는 방법으로 그 도메인을 재정의할 수 있습니다.

- 이름 서버 삭제:

```
dnsconfig roots delete <ns_domain> [ns_name]
```



참고 삭제할 때 ns_name을 지정하지 않을 경우 해당 도메인의 모든 이름 서버가 제거됩니다.

- 모든 DNS 설정을 지우고 시스템에서 인터넷 루트 서버를 사용하도록 자동으로 구성:

```
dnsconfig roots
```

현재 DNS 설정 표시:

```
dnsconfig print
```

예

각 사용자 지정 DNS 서버에 다음 정보가 필요합니다.

- 호스트 이름
- IP 주소
- 권한 대상 도메인(대체 서버만)

dnsconfig 명령에서 4가지 하위 명령을 사용할 수 있습니다.

표 4: **dnsconfig** 명령의 하위 명령

Syntax	설명
new	특정 도메인에 사용할 대체 DNS 서버 또는 로컬 DNS 서버를 추가합니다.
delete	대체 서버 또는 로컬 DNS 서버를 제거합니다.
edit	대체 서버 또는 로컬 DNS 서버를 수정합니다.
setup	인터넷 루트 DNS 서버 또는 로컬 DNS 서버로 전환합니다.

```
mail3.example.com> dnsconfig
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[1]> setup
Do you want the Gateway to use the Internet's root DNS servers or would you like
it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use own DNS cache servers
[1]> 1
Choose the IP interface for DNS traffic.
1. Auto
2. Management (10.92.149.70/24: mail3.example.com)
[1]>
Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>
Enter the minimum TTL in seconds for DNS cache.
```

```
[1800]>
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

특정 도메인을 위한 대체 DNS 서버 추가

특정 로컬 도메인을 제외하고 모든 DNS 쿼리에서 인터넷 루트 서버를 사용하도록 어플라이언스를 구성할 수 있습니다.

```
mail3.example.com> dnsconfig
Currently using the Internet root DNS servers.
No alternate authoritative servers configured.
Choose the operation you want to perform:
- NEW - Add a new server.
- SETUP - Configure general settings.
[]> new
Please enter the domain this server is authoritative for. (Ex: "com").
[]> example.com
Please enter the fully qualified hostname of the DNS server for the domain "example.com".
(Ex: "dns.example.com").
[]> dns.example.com
Please enter the IP address of dns.example.com.
[]> 10.1.10.9
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

자체 DNS 캐시 서버 사용

자체 DNS 캐시 서버를 사용하도록 어플라이언스를 구성할 수 있습니다.

```
mail3.example.com> dnsconfig
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]> setup
Do you want the Gateway to use the Internet's root DNS servers or would you like
it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use own DNS cache servers
[1]> 2
Please enter the IP address of your DNS server.
Separate multiple IPs with commas.
```

```
[ ]> 10.10.200.03
Please enter the priority for 10.10.200.3.
A value of 0 has the highest priority.
The IP will be chosen at random if they have the same priority.
[0]> 1
Choose the IP interface for DNS traffic.
1. Auto
2. Management (192.168.42.42/24)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>
Enter the minimum TTL in seconds for DNS cache.
[1800]>
Currently using the local DNS cache servers:
1. Priority: 1 10.10.200.3
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[ ]>
```

dnsflush

설명

DNS 캐시에서 모든 항목을 지웁니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> dnsflush
Are you sure you want to clear out the DNS cache? [N]> Y
```

dnshostprefs

설명

IPv4/IPv6 DNS 환경 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> dnshostprefs
Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]> new
Enter the domain you wish to configure.
[]> example.com
How should the appliance sort IP addresses for this domain?
1. Prefer IPv4
2. Prefer IPv6
3. Require IPv4
4. Require IPv6
[2]> 3
Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]> setdefault
How should the appliance sort IP addresses?
1. Prefer IPv4
2. Prefer IPv6
3. Require IPv4
4. Require IPv6
[2]> 1
Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]>
```

dnslistconfig

설명

DNS 목록 서비스 지원을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> dnslistconfig
Current DNS List Settings:
Negative Response TTL: 1800 seconds
DNS List Query Timeout: 3 seconds
Choose the operation you want to perform:
- SETUP - Configure general settings.
[]> setup
Enter the cache TTL for negative responses in seconds:
```

```
[1800]> 1200
Enter the query timeout in seconds:
[3]>
Settings updated.
Current DNS List Settings:
Negative Response TTL: 1200 seconds
DNS List Query Timeout: 3 seconds
Choose the operation you want to perform:
- SETUP - Configure general settings.
[]>
```

dnslisttest

설명

DNS 기반 목록 서비스를 위해 DNS 조회를 테스트합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> dnslisttest
Enter the query server name:
[]> mail4.example.com
Enter the test IP address to query for:
[127.0.0.2]> 10.10.1.11
Querying: 10.10.1.11.mail4.example.com
Result: MATCHED
```

dnsstatus

설명

DNS 통계를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> dnsstatus
```

```
Status as of: Mon Apr 18 10:58:07 2005 PDT
Counters:
DNS Requests          1,115      1,115      1,115
Network Requests     186        186        186
Cache Hits           1,300      1,300      1,300
Cache Misses          1           1           1
Cache Exceptions      0           0           0
Cache Expired        185        185        185
```

How-Tos 위젯을 사용하여 사용자 경험 향상

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [howtoupdate, 87 페이지](#)
- [howtostatus, 87 페이지](#)

howtoupdate

설명

howtoupdate 명령은 How-Tos 구성 요소를 수동으로 업데이트하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help howtoupdate` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

다음 예에서는 howtoupdate 명령을 사용하여 How-Tos 구성 요소를 수동으로 업데이트할 수 있습니다.

```
mail.example.com > howtoupdate
Requesting update of How-Tos component
```

howtostatus

설명

howtostatus 명령은 How-Tos 구성 요소의 현재 버전을 표시하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help howtostatus` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

다음 예에서는 `howtostatus` 명령을 사용하여 How-Tos 구성 요소의 현재 버전을 볼 수 있습니다.

```
mail.example.com > howtostatus
```

```
Component                Version Last Updated
How-Tos                   1.0 4 Jul 2018 04:22 (GMT +00:00)
```

일반 관리 및 문제 해결

This section contains the following CLI commands:

- [addressconfig, 89 페이지](#)
- [adminaccessconfig, 90 페이지](#)
- [certconfig, 96 페이지](#)
- [날짜, 100 페이지](#)
- [진단, 101 페이지](#)
- [diskquotaconfig, 106 페이지](#)
- [ecconfig, 107 페이지](#)
- [ecstatus, 108 페이지](#)
- [ecupdate, 108 페이지](#)
- [encryptionconfig, 109 페이지](#)
- [encryptionstatus, 112 페이지](#)
- [encryptionupdate, 112 페이지](#)
- [enginestatus, 113 페이지](#)
- [featurekey, 114 페이지](#)
- [featurekeyconfig, 115 페이지](#)
- [generalconfig, 115 페이지](#)
- [healthcheck, 116 페이지](#)
- [healthconfig, 117 페이지](#)
- [ntpconfig, 118 페이지](#)
- [portalregistrationconfig, 119 페이지](#)
- [reboot, 120 페이지](#)
- [repengstatus, 120 페이지](#)
- [resume, 120 페이지](#)
- [resumedel, 121 페이지](#)
- [resumelister, 121 페이지](#)
- [회선, 122 페이지](#)
- [settime, 123 페이지](#)

- [settz, 123 페이지](#)
- [shutdown, 124 페이지](#)
- [sshconfig, 125 페이지](#)
- [status, 129 페이지](#)
- [supportrequest, 130 페이지](#)
- [supportrequeststatus, 132 페이지](#)
- [supportrequestupdate, 132 페이지](#)
- [suspend, 132 페이지](#)
- [suspenddel, 133 페이지](#)
- [suspendlistener, 133 페이지](#)
- [tcpsservices, 134 페이지](#)
- [techsupport, 135 페이지](#)
- [tlsverify, 136 페이지](#)
- [trace, 136 페이지](#)
- [trackingconfig, 138 페이지](#)
- [updateconfig, 139 페이지](#)
- [updatenow, 143 페이지](#)
- [upgrade, 145 페이지](#)
- [버전, 144 페이지](#)
- [wipedata, 144 페이지](#)

가상 어플라이언스 관리, 323 페이지도 참고하십시오.

addressconfig

설명

addressconfig 명령은 From: 주소 헤더를 구성할 때 사용합니다. From: 주소의 표시 이름, 사용자 이름, 도메인 이름을 지정할 수 있습니다. 도메인 이름에 가상 게이트웨이 도메인을 사용하도록 선택할 수도 있습니다. 다음과 같은 상황에서는 AsyncOS에서 생성하는 메일에 **addressconfig** 명령을 사용합니다.

- 안티바이러스 알림
- 반송
- DMARC 피드백 보고서
- 알림(notify() 및 notify-copy()) 필터 작업)
- 격리 메시지(및 격리 관리의 “Send Copy”)
- 보고서
- 기타 모든 메시지

다음 예에서는 알림의 From: 주소가 Mail Delivery System [MAILER-DAEMON@domain](기본값)에서 Notifications [Notification@example.com]으로 바뀝니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> addressconfig
Current anti-virus from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current bounce from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current notify from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current quarantine from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current DMARC reports from: "DMARC Feedback" <MAILER-DAEMON@domain>
Current all other messages from: "Mail Delivery System" <MAILER-DAEMON@domain>
Choose the operation you want to perform:
- AVFROM - Edit the anti-virus from address.
- BOUNCEFROM - Edit the bounce from address.
- NOTIFYFROM - Edit the notify from address.
- QUARANTINEFROM - Edit the quarantine bcc from address.
- DMARCFROM - Edit the DMARC reports from address.
- OTHERFROM - Edit the all other messages from address.
[]> notifyfrom
Please enter the display name portion of the "notify from" address
["Mail Delivery System"]> Notifications
Please enter the user name portion of the "notify from" address
[MAILER-DAEMON]> Notification
Do you want the virtual gateway domain used for the domain? [Y]> n
Please enter the domain name portion of the "notify from" address
[]> example.com
Current anti-virus from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current bounce from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current notify from: Notifications <Notification@example.com>
Current quarantine from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current DMARC reports from: "DMARC Feedback" <MAILER-DAEMON@domain>
Current all other messages from: "Mail Delivery System" <MAILER-DAEMON@domain>
Choose the operation you want to perform:
- AVFROM - Edit the anti-virus from address.
- BOUNCEFROM - Edit the bounce from address.
- NOTIFYFROM - Edit the notify from address.
- QUARANTINEFROM - Edit the quarantine bcc from address.
- DMARCFROM - Edit the DMARC reports from address.
- OTHERFROM - Edit the all other messages from address.
[]>
```

adminaccessconfig

설명

다음을 구성할 때 **adminaccessconfig** 명령을 사용합니다.

- 관리자를 위한 로그인 메시지(배너)
- 어플라이언스 관리 인터페이스를 위한 IP 기반 액세스
- 웹 인터페이스 교차 사이트 요청 위조 방지

- HTTP 요청에 호스트 헤더를 사용하는 옵션
- 웹 인터페이스 및 CLI 세션 휴면 시간 초과
- 최대 HTTP 헤더 크기.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

adminaccessconfig 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 모든 IP 주소에 대한 액세스를 허용할지 아니면 특정 IP 주소/서브넷/범위로 액세스를 한정할지 선택합니다.

```
adminaccessconfig ipaccess <all/restrict/proxyonly/proxy>
```

- 새 IP 주소/서브넷/범위 추가

```
adminaccessconfig ipaccess new <address>
```

- 기존 IP 주소/서브넷/범위 수정

```
adminaccessconfig ipaccess edit <oldaddress> <newaddress>
```

- 기존 IP 주소/서브넷/범위 삭제

```
adminaccessconfig ipaccess delete <address>
```

- IP 주소/서브넷/범위의 목록 인쇄

```
adminaccessconfig ipaccess print
```

- 기존 IP 주소/서브넷/범위 모두 삭제

```
adminaccessconfig ipaccess clear
```

- 로그인 배너 인쇄

```
adminaccessconfig banner print
```

- 어플라이언스의 파일에서 로그인 배너 가져오기

```
adminaccessconfig banner import <filename>
```

- 기존 로그인 배너 삭제

```
adminaccessconfig banner clear
```

- 환영 배너 인쇄

```
adminaccessconfig welcome print
```

- 어플라이언스의 파일에서 환영 배너 가져오기

```
adminaccessconfig welcome import <filename>
```

- 기존 환영 배너 삭제

```
adminaccessconfig welcome clear
```

- 환영 배너 내보내기

```
adminaccessconfig welcome export <filename>
```

- 허용된 프록시 IP 주소 추가

```
adminaccessconfig ipaccess proxylist new <address>
```

- 허용된 프록시 IP 주소 수정

```
adminaccessconfig ipaccess proxylist edit <oldaddress> <newaddress>
```

- 허용된 프록시 IP 주소 삭제

```
adminaccessconfig ipaccess proxylist delete <address>
```

- 기존의 허용된 프록시 IP 주소 모두 삭제

```
adminaccessconfig ipaccess proxylist clear
```

- 원래의 IP 주소를 포함하는 헤더 이름 구성

```
adminaccessconfig ipaccess proxy-header <header name>
```

- 웹 인터페이스 교차 사이트 요청 위조 방지 활성화 또는 비활성화


```
adminaccessconfig csrf <enable|disable>
```

- 웹 인터페이스 교차 사이트 요청 위조 방지가 활성화되었는지 확인

```
adminaccessconfig csrf print
```

- 웹 인터페이스 세션 시간 초과 구성

```
adminaccessconfig timeout gui <value>
```

- CLI 세션 시간 초과 구성

```
adminaccessconfig timeout cli <value>
```

예 - 네트워크 액세스 목록 구성

사용자가 어떤 IP 주소에서 ESA에 액세스하는지 제어할 수 있습니다. 사용자는 정의된 액세스 목록에 포함된 IP 주소의 시스템에서 어플라이언스에 액세스할 수 있습니다. 네트워크 액세스 목록을 생성할 때 IP 주소, 서브넷 또는 CIDR 주소를 지정할 수 있습니다.

AsyncOS는 네트워크 액세스 목록에 현재 시스템의 IP 주소를 포함하지 않으면 경고를 표시합니다. 현재 시스템의 IP 주소가 목록에 없을 경우 변경 사항을 커밋한 다음에는 어플라이언스에 액세스할 수 없습니다.

다음 예에서는 어플라이언스에 대한 네트워크 액세스가 두 IP 주소 세트에 한정됩니다.

```
mail.example.com> adminaccessconfig
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSize - Configure maximum HTTP header field size.
[ ]> ipaccess
Current mode: Allow All.
Please select the mode:
- ALL - All IP addresses will be allowed to access the administrative interface.
- RESTRICT - Specify IP addresses/Subnets/Ranges to be allowed access.
- PROXYONLY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy.
- PROXY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy or directly.
[ ]> restrict
List of allowed IP addresses/Subnets/Ranges:
Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
[ ]> new
Please enter IP address, subnet or range.
[ ]> 192.168.1.2-100
List of allowed IP addresses/Subnets/Ranges:
1. 192.168.1.2-100
Choose the operation you want to perform:
```

```

- NEW - Add a new IP address/subnet/range.
- EDIT - Modify an existing entry.
- DELETE - Remove an existing entry.
- CLEAR - Remove all the entries.
[> new
Please enter IP address, subnet or range.
[> 192.168.255.12
List of allowed IP addresses/Subnets/Ranges:
1. 192.168.1.2-100
2. 192.168.255.12
Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
- EDIT - Modify an existing entry.
- DELETE - Remove an existing entry.
- CLEAR - Remove all the entries.
[>
Warning: The host you are currently using [72.163.202.175] is not included in the User
Access list. Excluding it will prevent your
host from connecting to the administrative interface. Are you sure you want to continue?
[N]> Y
Current mode: Restrict.
Please select the mode:
- ALL - All IP addresses will be allowed to access the administrative interface.
- RESTRICT - Specify IP addresses/Subnets/Ranges to be allowed access.
- PROXYONLY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy.
- PROXY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy or directly.
[>

```

예 - 로그인 배너 구성

사용자가 SSH, Telnet, FTP 또는 웹 UI를 통해 어플라이언스에 로그인을 시도할 때 "로그인 배너"라는 메시지를 표시하도록 Email Security Appliance를 구성할 수 있습니다. 로그인 배너는 사용자 정의할 수 있는 텍스트로 GUI에서 로그인 프롬프트의 오른쪽과 CLI의 로그인 프롬프트 위에 나타납니다. 로그인 배너를 사용하여 내부 보안 정보나 어플라이언스에 대한 모범 사례를 표시할 수 있습니다. 예를 들어, 어플라이언스의 무단 사용이 금지되어 있다고 알려주거나 사용자에게 의한 어플라이언스의 검토 변경에 대한 조직의 권리에 관한 자세한 경고문을 알려주는 간단한 메모를 작성할 수 있습니다.

로그인 배너의 최대 길이는 80X25 콘솔에 맞는 2000자입니다. 로그인 배너는 어플라이언스의 /data/pub/configuration 디렉토리에 있는 파일에서 가져올 수 있습니다. 배너를 작성한 후 변경 사항을 커밋하십시오.

다음 예에서는 "Use of this system in an unauthorized manner is prohibited" 로그인 배너가 어플라이언스에 추가되었습니다.

```

mail.example.com> adminaccessconfig
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSize - Configure maximum HTTP header field size.
[> banner
A banner has not been defined.
Choose the operation you want to perform:
- NEW - Create a banner to display at login.
- IMPORT - Import banner text from a file.

```

```

[ ]> new
Enter or paste the banner text here. Enter CTRL-D on a blank line to end.
Use of this system in an unauthorized manner is prohibited.
^D
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[ ]> banner
Banner: Use of this system in an unauthorized manner is prohibited.
Choose the operation you want to perform:
- NEW - Create a banner to display at login.
- IMPORT - Import banner text from a file.
- DELETE - Remove the banner.
[ ]>

```

예 - 웹 인터페이스 및 CLI 세션 시간 초과 구성

다음 예에서는 웹 인터페이스 및 CLI 세션 시간 초과를 32분으로 설정합니다.



참고

CLI 세션 시간 초과는 SSH(Secure Shell), SCP, 직접 직렬 연결을 사용하는 연결에만 적용됩니다. CLI 세션의 시간 초과 시점에 커밋되지 않은 구성 변경사항은 손실됩니다. 따라서 구성을 변경한 후 즉시 구성 변경사항을 커밋해야 합니다.

```

mail.example.com> adminaccessconfig
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSIZE - Configure maximum HTTP header field size.
[ ]> timeout
Enter WebUI inactivity timeout(in minutes):
[30]> 32
Enter CLI inactivity timeout(in minutes):
[30]> 32
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[ ]>
mail.example.com> commit
Please enter some comments describing your changes:
[ ]> Changed WebUI and CLI session timeout values
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Wed Mar 12 08:03:21 2014 GMT

```



참고 변경을 커밋한 후 다음 로그인 과정에서 새 CLI 세션 시간 초과가 적용됩니다.

certconfig

설명

보안 인증서 및 키를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예 - 인증서에 붙여넣기

다음 예에서는 인증서 및 개인 키에 붙여넣는 방법으로 인증서를 설치합니다.

```
mail3.example.com> certconfig
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate
List of Certificates
-----
Name          Common Name          Issued By          Status          Remaining
-----
Demo          Cisco Appliance Demo Cisco Appliance Demo Active          3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- PRINT - View certificates assigned to services
[]> paste
Enter a name for this certificate profile:
> partner.com
Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgAxCzAJBgNVBAYTA1BURRMwEQYD
VQOIEwprDwVlbnNsYW5kMQ8wDQYDVQQHEwZMaXN1b2ExFzAVBgNVBAoTDk5ldXJv
bmlvLlCBMzZGEuMRgwFgYDVQQLEw9EZXR1bnZvbHJpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCsGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MTk5MDk2NDk5NDIOM1oXDTk2M2AwNTAzNDIOM1owgAxCzAJBgNVBAYTA1BURRMw
EQYDVQOIEwprDwVlbnNsYW5kMQ8wDQYDVQQHEwZMaXN1b2ExFzAVBgNVBAoTDk5l
dXJvbm1vLlCBMzZGEuMRgwFgYDVQQLEw9EZXR1bnZvbHJpbWVudG8xGzAZBgNVBAMT
EmJydXR1cy5uZXVyb25pby5wdDEbMBkGCsGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MFwwDQYJKoZIhvcNAQEEBQADSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTdlkjNw
L4lYKbpzZlmC5beaQXeQ2RmGMTXU+mDvuqItjVHOK3DvPK71TcSGftUCAWEAATAN
BgkqhkiG9w0BAQQFAANBAFqPEKfjk6T6CKTHvaQeEAsX0/8YHPHqH/9AnhSjrWuX
9EBcOn6bVGHn7XaXd6sJ7dym9sbsWxb+pJdurnkxjx4=
-----END CERTIFICATE-----
.
```

```

C=PT,ST=Queensland,L=Lisboa,O=Neuronio,
Lda.,OU=Desenvolvimento,CN=brutus.partner.com,emailAddress=admin@example.com
Paste private key in PEM format (end with '.'):
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIbAAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNwL41YKbpzlmC5beaQXeQ
2RmGMTXU+mDvuqItjVHOK3DvPK71TcSGftUCAwEAAQJBALjkK+jc2+iihI98riEF
oudmkNziSRTYjnwjx8mCoAjPWviB3c742eO3FG4/soiljd9A5alihEOXFUzloenr
8IECIQD3B5+0l+68BA/6d76iUNqAAV8djGTzvxnCxyenxPQydQIhAMXt4trUI3nc
a+U8YL2HPFA3gmhBsSICbq2OptOCnM7hAiEA6Xi3JIQECob8Ywkrj29DU3/4WYD7
WLPgsQpwo1GuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IzmxcLpRcpslpeWBBAiEA
6/5B8J0GHdJq89FHwEG/H2eVVUYu5y/aD6sgcm+0Avg=
-----END RSA PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
partner.c brutus.partner.com brutus.partner     Active          30 days
Demo         Cisco Appliance Demo Cisco Appliance Demo Active          3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Installed certificate and key for receiving, delivery, and https
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

예 - 자체 서명 인증서 생성

다음 예에서는 자체 서명 인증서를 생성합니다.

```

mail3.example.com> certconfig
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
partner.c brutus.neuronio.pt brutus.neuronio.pt Expired          -4930
days
Demo         Cisco Appliance Demo Cisco Appliance Demo Active          3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate

```

```

- PRINT - View certificates assigned to services
[> new
1. Create a self-signed certificate and CSR
2. Create a self-signed SMIME certificate and CSR
[1]> 1
Enter a name for this certificate profile:
> example.com
Enter Common Name:
> example.com
Enter Organization:
> Example
Enter Organizational Unit:
> Org
Enter Locality or City:
> San Francisco
Enter State or Province:
> CA
Enter Country (2 letter code):
> US
Duration before expiration (in days):
[3650]>
1. 1024
2. 2048
Enter size of private key:
[2]>
Do you want to view the CSR? [Y]> y
-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwADELMAkGA1UEBhMCVVMxZDASBgNVBAMTC2V4YW1wbGUuY29t
MRYwFAYDVQQHEw1TYW4gRnJhbmNpc29jMRAwDgYDVQQKEWdleGFtcGxlMQswCQYD
VQQIEwJkQTEEMMAoGA1UECmM3JnMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEANwamZyX7VgTZka/x1I5HHrN9V2MPKXoLq7FjzUtiIDwznElrKIuJovw
Svonle6GvFlUHfjv8B3WobOzk5Ny6btKjwPrBfaY+qr7rzM41AQKHM+P61+lZnPU
P05N9RCkLP4XsUuyY6Ca1WLTiPIgaq2fR8Y0JX/kesZcGOqlde66pN+xJIHHYadD
oopOgqi6SLNfAzJu/HEu/fnSujG4nhF0ZG1OpVUx4fg33NwZ4wV10XBk3GrOjbbA
ih9ozAwfNzxb57amtXEJk+pW+co3uEHLJIOPdih9SHzn/UUV4hiu8rSQR19sDApp
kfdWcfaDLF9tnQJPWSYoCh0USgCc8QIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEB
AGiVhyMAZuHSv9yA08kJCmrgO89yRlnDUXDDo6IrODVKx4hHTiOanOPulnsThSvH
7xv4xR35T/QV0U3yPrL6bJbbwMySOLIRTjsUcwZnJOE1xMM5EkBM2BOI5rs4l59g
FhHVejhG1LyyUDL0U82wsSLMqLFH1IT63tzwVmRiIXmAu/lHYci3+vctb+sopnN1
lY10IuJ+EqqWnrRBNnKXLtdXkzhELOd8vZEgSAfBWyjZ2mECzC7SG3evqkw/OGlK
AilNXHayiGjeY+UfWzF/HBSekSjtQu6hIv6JpBSY/MnYU4t1lExqD+GX3lru4xc4
zDas2rS/Pbpn73Lf503nmsw=
-----END CERTIFICATE REQUEST-----
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
example.c     example.com          example.com        Valid           3649 days
partner.c     brutus.partner.com   brutus.partner.com Valid           30 days
Demo         Cisco Appliance Demo Cisco Appliance Demo Active           3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[>

```

예 - 자체 서명 S/MIME 서명 인증서 생성

다음 예에서는 메시지 서명을 위해 자체 서명 S/MIME 인증서를 생성하는 방법을 보여줍니다.

```

vm10esa0031.qa> certconfig
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
Demo          Cisco Appliance Demo Cisco Appliance Demo Active          3329 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- PRINT - View certificates assigned to services
[]> new
1. Create a self-signed certificate and CSR
2. Create a self-signed SMIME certificate and CSR
[1]> 2
Enter a name for this certificate profile:
> smime_signing
Enter Common Name:
> CN
Enter Organization:
> ORG
Enter Organizational Unit:
> OU
Enter Locality or City:
> BN
Enter State or Province:
> KA
Enter Country (2 letter code):
> IN
Duration before expiration (in days):
[3650]>
1. 1024
2. 2048
Enter size of private key:
[2]>
Enter email address for 'subjectAltName' extension:
[]> admin@example.com
Add another member? [Y]> n
Begin entering domain entries for 'subjectAltName'.
Enter the DNS you want to add.
[]> domain.com
Add another member? [Y]> n
Do you want to view the CSR? [Y]> n
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
smime_sig     CN                   CN                 Valid           3649 days
Demo          Cisco Appliance Demo Cisco Appliance Demo Active          3329 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>

```

날짜

설명

현재 날짜 및 시간을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> date
Tue Mar 10 11:30:21 2015 GMT
```

daneverify

- [설명, 100 페이지](#)
- [Usage\(사용\), 100 페이지](#)
- [예, 100 페이지](#)

설명

지정된 도메인에 대해 DANE가 지원되는지 여부를 확인합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help daneverify` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

다음 예에서는 `daneverify` 명령을 사용하여 지정된 도메인에 대한 DANE 지원을 확인할 수 있습니다.

```
mail3.example.com> daneverify
Enter the DANE domain to verify against: []> example-dane.net
Trying DANE MANDATORY for example-dane.net
SECURE MX RECORD found for example-dane.net
SECURE A record (10.10.1.198) found for MX(mail.example.com.cs2.test-dane.net) in
example-dane.net
SECURE TLSA Record found for MX(mail.example.com.cs2.test-dane.net) in example-dane.net TLS
```



```

connection established: protocol TLSv1.2, cipher DHE-RSA-AES128-SHA256.
Certificate verification successful for TLSA
record(030101329aad19cfb5a0bb8d3b99c67dd1282a4dcdf67bd9c4efc08578657065fe7504)
TLS connection succeeded example-dane.net.
DANE_SUCCESS for example-dane.net
DANE verification completed.
    
```

진단

설명

다음 용도로 **diagnostic** 명령을 사용합니다.

- 다양한 유틸리티를 사용하여 하드웨어 및 네트워크 문제 트러블슈팅
- RAID 상태 확인
- ARP 캐시 표시
- LDAP, DNS, ARP 캐시 지우기
- SMTP 테스트 메시지 보내기
- 어플라이언스에서 활성화된 서비스 엔진 다시 시작 및 상태 보기.

diagnostic 명령 사용

diagnostic 하위 메뉴에서 다음 명령을 사용할 수 있습니다.

표 5: **diagnostic** 하위 명령

옵션	하위 명령	사용 가능
RAID	1. 디스크 확인 실행	C30 및 C60에서만
	2. 진행 중인 작업 모니터링	
	3. 디스크 확인 결과 표시	
DISK_USAGE (사용 중지)	하위 명령 없음	이 명령은 더 이상 사용하지 않습니다. 그 대신 diskquotaconfig 명령을 사용합니다.
NETWORK	FLUSH	C Series, X Series, M Series
	ARPSHOW	
	SMTTPING	
	TCPDUMP	
REPORTING	DELETEDB	C Series, X Series, M Series
	DISABLE	

옵션	하위 명령	사용 가능
TRACKING	DELETEDB	C Series, X Series, M Series
	DEBUG	
RELOAD	하위 명령 없음	C Series, X Series, M Series
서비스	RESTART 상태	C Series, X Series, M Series

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

diagnostic 명령의 배치 형식은 RAID 상태를 확인하고 캐시를 지우고 ARP 캐시의 내용을 표시하는 데 사용할 수 있습니다. 배치 명령으로 실행하려면 다음 형식을 사용합니다.

다음 작업을 수행하려면 배치 형식을 사용합니다.

- RAID 상태 확인

```
diagnostic raid
```

- ARP 캐시의 내용 표시

```
diagnostic network arpshow
```

- NDP 캐시의 내용 표시

```
diagnostic network ndpshow
```

- LDAP, DNS, ARP, NDP 캐시 지우기

```
diagnostic network flush
```

- 보고 데이터베이스 재설정 및 삭제

```
diagnostic reporting deletedb
```

- 보고 데몬 활성화

```
diagnostic reporting enable
```

- 보고 데몬 비활성화

```
diagnostic reporting disable
```

- 추적 데이터베이스 재설정 및 삭제

```
diagnostic tracking deletedb
```

- 초기 제조업체 값으로 컨피그레이션 재설정

```
diagnostic reload
```

예: 캐시 표시 및 지우기

다음 예에서는 **diagnostic** 명령을 사용하여 ARP 캐시의 내용을 표시하고 모든 네트워크 관련 캐시를 플러시합니다.

```
mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[ ]> network
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTTPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[ ]> arpshow
System ARP cache contents:
(10.76.69.3) at 00:1e:bd:28:97:00 on em0 expires in 1193 seconds [ethernet]
(10.76.69.2) at 00:1e:79:af:f4:00 on em0 expires in 1192 seconds [ethernet]
(10.76.69.1) at 00:00:0c:9f:f0:01 on em0 expires in 687 seconds [ethernet]
(10.76.69.149) at 00:50:56:b2:0e:2b on em0 permanent [ethernet]
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTTPING - Test a remote SMTP server.
```

예: 다른 메일 서버와의 연결 확인

```

- TCPDUMP - Dump ethernet packets.
[ ]> flush
Flushing LDAP cache.
Flushing DNS cache.
Flushing system ARP cache.
10.76.69.3 (10.76.69.3) deleted
10.76.69.2 (10.76.69.2) deleted
10.76.69.1 (10.76.69.1) deleted
10.76.69.149 (10.76.69.149) deleted
Flushing system NDP cache.
fe80::250:56ff:feb2:e2d%em2 (fe80::250:56ff:feb2:e2d%em2) deleted
fe80::250:56ff:feb2:e2c%em1 (fe80::250:56ff:feb2:e2c%em1) deleted
fe80::250:56ff:feb2:e2b%em0 (fe80::250:56ff:feb2:e2b%em0) deleted
Network reset complete.

```

예: 다른 메일 서버와의 연결 확인

다음 예에서는 **diagnostics**를 사용하여 다른 메일 서버와의 연결을 확인합니다. 메시지를 보내거나 서버를 **ping**하여 메일 서버를 테스트할 수 있습니다.

```

mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[ ]> network
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTTPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[ ]> smtpping
Enter the hostname or IP address of the SMTP server:
[mail.example.com]> mail.com
The domain you entered has MX records.
Would you like to select an MX host to test instead? [Y]> y
Select an MX host to test.
1. mx00.gmx.com
2. mx01.gmx.com
[1]>
Select a network interface to use for the test.
1. Management
2. auto
[2]> 1
Do you want to type in a test message to send? If not, the connection will be tested but
no email will be sent. [N]>
Starting SMTP test of host mx00.gmx.com.
Resolved 'mx00.gmx.com' to 74.208.5.4.
Unable to connect to 74.208.5.4.

```

예: 초기 제조업체 값으로 어플라이언스 컨피그레이션 재설정

다음 예에서는 어플라이언스 컨피그레이션을 초기 제조업체 값으로 재설정하는 방법을 보여줍니다.

```

mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.

```

```

- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[]> reload
This command will remove all user settings and reset the entire device.
If this is a Virtual Appliance, all feature keys will be removed,
and the license must be reapplied.
Are you sure you want to continue? [N]> Y
Are you *really* sure you want to continue? [N]> Y
Do you want to wipe also? [N]> Y

```

서비스 엔진 다시 시작 및 상태 보기

CLI에서 `diagnostic > servicessub` 명령을 사용하여 다음 작업을 수행할 수 있습니다.

- 어플라이언스를 재부팅하지 않고도 어플라이언스에서 활성화된 서비스 엔진을 다시 시작합니다.
- 어플라이언스에서 활성화된 서비스 엔진의 상태를 봅니다.

예: DLP 엔진의 상태 보기

다음 예에서는 `services` 명령을 사용하여 어플라이언스에서 활성화된 DLP 엔진의 상태를 확인합니다.

```

mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> dlp

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

Cisco Data Loss Prevention has been up for 3s.

```

예: 그레이메일 엔진 다시 시작

다음 예에서는 `services` 명령을 사용하여 어플라이언스에 활성화된 그레이메일을 다시 시작합니다.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> graymail

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart
```

diskquotaconfig

보고 및 추적, 격리, 로그 파일, 패킷 캡처, 컨피그레이션 파일을 위한 디스크 공간 할당을 보거나 구성합니다.

이 기능에 대한 자세한 내용은 *AsyncOS for Cisco Email Security Appliance* 사용 설명서를 참조하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

```
diskquotaconfig <feature> <quota> [<feature> <quota> [<feature> <quota>[<feature> <quota>]]]
```

<feature>에 유효한 값은 `eq`, `pvo`, `tracking`, `reporting`입니다.

<quota>에 유효한 값은 정수입니다.

예

```
mail.example.com> diskquotaconfig
Service
-----
Spam Quarantine (EUQ)                1          1
Policy, Virus & Outbreak Quarantines 1          3
Reporting                            5          10
Tracking                             1          10
Miscellaneous Files                   5          30
    System Files Usage : 5 GB
    User Files Usage : 0 GB
Total                                13         54 of 143
Choose the operation you want to perform:
- EDIT - Edit disk quotas
[]> edit
Enter the number of the service for which you would like to edit disk quota:
1. Spam Quarantine (EUQ)
2. Policy, Virus & Outbreak Quarantines
3. Reporting
4. Tracking
5. Miscellaneous Files
[1]> 1
Enter the new disk quota -
[1]> 1
Disk quota for Spam Quarantine (EUQ) changed to 1
Service
-----
Spam Quarantine (EUQ)                1          1
Policy, Virus & Outbreak Quarantines 1          3
Reporting                            5          10
Tracking                             1          10
Miscellaneous Files                   5          30
    System Files Usage : 5 GB
    User Files Usage : 0 GB
Total                                13         54 of 143
Choose the operation you want to perform:
- EDIT - Edit disk quotas
[]>
```

ecconfig

URL 필터링 기능에 사용할 인증서를 얻는 데 쓰이는 등록 클라이언트를 설정하거나 지웁니다.

이 명령을 사용할 때는 반드시 Cisco 팀의 지원을 받으십시오.

항목은 <hostname:port> 또는 <IPv4 address:port> 형식이어야 합니다. 포트는 선택 사항입니다.

기본 서버를 지정하려면 `ecconfig server default`를 입력합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 클러스터의 모든 레벨에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

- 비 기본 등록 클라이언트 서버 지정:

```
> ecconfig server <server_name:port>
```

기본 등록 클라이언트 서버 사용:

```
> ecconfig server default
```

예

```
mail.example.com> ecconfig
Enrollment Server: Not Configured (Use Default)
Choose the operation you want to perform:
- SETUP - Configure the Enrollment Server
[ ]> setup
Do you want to use non-default Enrollment server?
WARNING: Do not configure this option without the assistance of Cisco Support.
Incorrect configuration can impact the services using certificates from the Enrollment
server. [N]> y
[ ]> 192.0.2.1
Choose the operation you want to perform:
- SETUP - Configure the Enrollment Server
[ ]>
```

ecstatus

URL 필터링에 사용할 인증서를 자동으로 얻는 데 쓰이는 등록 클라이언트의 현재 버전을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> ecstatus
Component                Version    Last Updated
Enrollment Client        1.0.2-046  Never updated
```

ecupdate

URL 필터링에 사용할 인증서를 자동으로 얻는 데 쓰이는 등록 클라이언트를 수동으로 업데이트합니다. 일반적으로 이 업데이트는 자동으로 이루어집니다. 이 명령을 사용할 때는 반드시 Cisco 팀의 지원을 받으십시오.

force 매개변수를 사용할 경우(ecupdate [force]) 변경 사항이 없을 때도 클라이언트가 업데이트됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

배치 형식

```
> ecupdate [force]
```

예

```
mail.example.com> ecupdate
Requesting update of Enrollment Client.
```

encryptionconfig

이메일 암호화를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 암호화 프로필을 수정합니다.

```
mail.example.com> encryptionconfig
IronPort Email Encryption: Enabled
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> setup
PXE Email Encryption: Enabled
Would you like to use PXE Email Encryption? [Y]>
WARNING: Increasing the default maximum message size(10MB) may result in
decreased performance. Please consult documentation for size recommendations
based on your environment.
Maximum message size for encryption: (Add a trailing K for kilobytes, M for
megabytes, or no letters for bytes.)
[10M]>
Enter the email address of the encryption account administrator
[administrator@example.com]>
IronPort Email Encryption: Enabled
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
```

```

[ ]> profiles
Proxy: Not Configured
Profile Name          Key Service          Proxied          Provision Status
-----
HIPAA                 Hosted Service       No               Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[ ]> edit
1. HIPAA
Select the profile you wish to edit:
[1]> 1
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated
Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLETT - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[ ]> security
1. High Security (Recipient must enter a passphrase to open the encrypted
message, even if credentials are cached ("Remember Me" selected).)
2. Medium Security (No passphrase entry required if recipient credentials are
cached ("Remember Me" selected).)
3. No passphrase Required (The recipient does not need a passphrase to open the
encrypted message.)
Please enter the envelope security level:
[1]> 1
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security

```

```

Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_$(date)T$(time).html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated
Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLETT - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]> forward
Would you like to enable "Secure Forward"? [N]> y
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: Yes
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_$(date)T$(time).html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated
Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLETT - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption

```

```
notification.
[]>
Proxy: Not Configured
Profile Name          Key Service          Proxied          Provision Status
-----
HIPAA                 Hosted Service       No              Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]>
IronPort Email Encryption: Enabled
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]>
```

encryptionstatus

설명

encryptionstatus 명령은 Email Security Appliance의 PXE 엔진 및 도메인 매핑 파일의 버전 그리고 이 구성 요소가 마지막으로 업데이트된 날짜와 시간을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> encryptionstatus
Component          Version  Last Updated
PXE Engine         6.7.1   17 Nov 2009 00:09 (GMT)
Domain Mappings File 1.0.0   Never updated
```

encryptionupdate

설명

encryptionupdate 명령은 Email Security Appliance의 PXE 엔진에 대한 업데이트를 요청합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> encryptionupdate
Requesting update of PXE Engine.
```

enginestatus

설명

enginestatus 명령은 어플라이언스에서 활성화된 다양한 엔진의 상태 및 CPU 사용량을 표시하는데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 **help enginestatus** 명령을 입력하여 온라인 도움말을 참고하십시오.

예

다음 예에서는 어플라이언스에서 활성화된 모든 엔진의 상태 및 CPU 사용량을 확인하는 방법을 보여 줍니다.

```
vm30esa0086.ibqa> enginestatus
Choose the operation you want to perform:
- GRAYMAIL - View Graymail engine status
- SOPHOS - View Sophos engine status
- CASE - View CASE engine status
- AMP - View AMP engine status
- MCAFEE - View McAfee engine status
- ALL - View status of All engines
[]> ALL
CASE Status: UP CPU: 0.0%
Component                Version                Last Updated
CASE Core Files           3.5.0-008             Never updated
CASE Utilities            3.5.0-008             Never updated
Structural Rules          3.3.1-009-20141210_214201  Never updated
Web Reputation DB         20141211_111021       Never updated
Web Reputation Rules      20141211_111021-20141211_170330  Never updated
Content Rules             unavailable            Never updated
Content Rules Update      unavailable            Never updated
SOPHOS Status: UP CPU: 0.0%
Component                Version                Last Updated
Sophos Anti-Virus Engine  3.2.07.365.2_5.30     Never updated
Sophos IDE Rules          0                      Never updated
GRAYMAIL Status: UP CPU: 0.0%
```

Component	Version	Last Updated
Graymail Engine +00:00) updated	01-392.68	N10 Nov 2016 07:08 (GMT)
Graymail Rules	01-392.68#121	Never updated
Graymail Tools	1.0.03	Never updated
MCAFEE Status: UP CPU: 0.0%		
Component	Version	Last Updated
McAfee Engine	5700	Never updated
McAfee DATs	7437	Never updated
AMP Status: UP CPU: 0.0%		
Component	Version	Last Updated
AMP Client Settings	1.0	Never updated
AMP Client Engine	1.0	Never updated

featurekey

설명

featurekey 명령은 시스템의 키에 의해 활성화된 모든 기능 및 키에 관한 정보를 나열합니다. 또한 키를 사용하여 기능을 활성화하거나 새 기능 키를 확인할 수도 있습니다.

가상 어플라이언스의 경우 [loadlicense, 323 페이지](#) 및 [showlicense, 324 페이지](#)도 참조하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 **featurekey** 명령을 사용하여 새 기능 키를 확인합니다.

```
mail3.example.com> featurekey
Module                               Quantity  Status   Remaining  Expiration Date
Outbreak Filters                     1        Active   28 days    Tue Feb 25 06:40:53
2014
IronPort Anti-Spam                   1        Dormant  30 days    Wed Feb 26 07:56:57
2014
Sophos Anti-Virus                    1        Active   26 days    Sun Feb 23 02:27:48
2014
Bounce Verification                  1        Dormant  30 days    Wed Feb 26 07:56:57
2014
Incoming Mail Handling                1        Active   20 days    Sun Feb 16 08:55:58
2014
IronPort Email Encryption             1        Dormant  30 days    Wed Feb 26 07:56:57
2014
Data Loss Prevention                  1        Active   25 days    Fri Feb 21 10:07:10
2014
McAfee                                1        Dormant  30 days    Wed Feb 26 07:56:57
2014
Choose the operation you want to perform:
- ACTIVATE - Activate a (pending) key.
- CHECKNOW - Check now for new feature keys.
[>] checknow
No new feature keys are available.
```

featurekeyconfig

설명

featurekeyconfig 명령으로 시스템에서 사용 가능한 키를 자동으로 다운로드하고 시스템의 키를 업데이트하도록 구성할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 **featurekeyconfig** 명령을 사용하여 **autoactivate**(자동 활성화) 및 **autocheck**(자동 확인) 기능을 활성화합니다.

```
mail3.example.com> featurekeyconfig
Automatic activation of downloaded keys: Disabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- SETUP - Edit feature key configuration.
[]> setup
Automatic activation of downloaded keys: Disabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- AUTOACTIVATE - Toggle automatic activation of downloaded keys.
- AUTOCHECK - Toggle automatic checking for new feature keys.
[]> autoactivate
Do you want to automatically apply downloaded feature keys? [N]> y
Automatic activation of downloaded keys: Enabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- AUTOACTIVATE - Toggle automatic activation of downloaded keys.
- AUTOCHECK - Toggle automatic checking for new feature keys.
[]> autocheck
Do you want to periodically query for new feature keys? [N]> y
Automatic activation of downloaded keys: Enabled
Automatic periodic checking for new feature keys: Enabled
```

generalconfig

설명

generalconfig 명령을 사용하여 브라우저 설정을 구성할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help generalconfig` 명령을 입력하여 인라인 도움말을 참고하십시오.

예 - Internet Explorer 호환성 모드 재정의 구성

다음 예에서는 IE 호환성 모드를 재정의하는 방법을 보여줍니다.

```
mail.example.com> generalconfig
Choose the operation you want to perform:
- IEVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]> ieoverride
  For better web interface rendering, we recommend that you enable Internet
  Explorer Compatibility Mode Override. However, if enabling this feature
  is against your organizational policy, you may disable this feature.
  Internet Explorer Compatibility Mode Override is currently disabled.
Would you like to enable Internet Explorer Compatibility Mode Override? [N]y
Choose the operation you want to perform:
- IEVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]>
```

healthcheck

설명

Email Security Appliance의 상태를 확인합니다. 상태 확인에서는 현재 상태 로그의 기록 데이터(최대 3개월분)를 분석하여 어플라이언스의 상태를 확인합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> healthcheck
Analyzing the system to determine current health of the system.
The analysis may take a while, depending on the size of the historical data.
System analysis is complete.
The analysis indicates that the system has experienced the following issue(s)recently:
Entered Resource conservation mode
Delay in mail processing
High CPU usage
High memory usage
Based on this analysis,
we recommend you to contact Cisco Customer Support before upgrading.
```


healthconfig

설명

어플라이언스의 다양한 상태 매개변수(예: CPU 사용량, 작업 큐의 최대 메시지 등)의 임계값을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> healthconfig
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> workqueue
Number of messages in the workqueue : 0
Current threshold on the workqueue size : 500
Alert when exceeds threshold : Disabled
Do you want to edit the settings? [N]> y
Please enter the threshold value for number of messages in work queue.
[500]> 550
Do you want to receive alerts if the number of messages in work queue exceeds
threshold value? [N]> n
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> cpu
Overall CPU usage : 0 %
Current threshold on the overall CPU usage: 85 %
Alert when exceeds threshold : Disabled
Do you want to edit the settings? [N]> y
Please enter the threshold value for overall CPU usage (in percent)
[85]> 90
Do you want to receive alerts if the overall CPU usage exceeds threshold value?[N]> n
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> swap
Number of pages swapped from memory in a minute : 0
Current threshold on the number of pages swapped from memory per minute : 5000
Alert when exceeds threshold : Disabled
Do you want to edit the settings? [N]> y
Please enter the threshold value for number of pages swapped from memory in a
minute.
[5000]> 5500
Do you want to receive alerts if number of pages swapped from memory in a
minute exceeds the threshold? [N]> n
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
```

```
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]>
```

ntpconfig

설명

ntpconfig 명령은 AsyncOS에서 NTP(Network Time Protocol)를 사용하여 시스템 시계를 다른 컴퓨터와 동기화하도록 구성합니다. NTP는 **settime** 명령을 사용하여 끌 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com>
ntpconfig
Currently configured NTP servers:
1. time.ironport.com
Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should originate.
- AUTH - Configure NTP authentication.
[]> new
Please enter the fully qualified hostname or IP address of your NTP server.
[]> ntp.example.com
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi
Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should
originate.
- AUTH - Configure NTP authentication.
[]> sourceint

When initiating a connection to an NTP server, the outbound IP address
used is chosen automatically.
If you want to choose a specific outbound IP address, please select
its interface name now.
1. Auto
2. Management (172.19.0.11/24: elroy.run)
3. PrivateNet (172.19.1.11/24: elroy.run)
4. PublicNet (172.19.2.11/24: elroy.run)
[1]> 1
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi
Choose the operation you want to perform:
- NEW - Add a server.
```

```

- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should originate.
- AUTH - Configure NTP authentication.
[]> auth

Would you like to enable NTP authentication? [N]>yes
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi
Authentication is on
Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should
originate.
- AUTH - Configure NTP authentication.

mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added new NTP server
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

portalregistrationconfig

Cisco 스팸 전송 추적 포털은 이메일 관리자가 조직의 스팸 전송을 추적하고 잘못 분류된 새 메시지를 Cisco에 보고하는 데 사용할 수 있는 웹 기반 도구입니다. 이 포털을 사용하려면 모든 어플라이언스에 공용 등록 ID가 있어야 합니다.

CLI에서 **portalregistrationconfig** 명령을 사용하여 등록 ID를 설정합니다. 어플라이언스가 클러스터의 일부가 아닌 경우 모든 어플라이언스에서 공용 등록 ID를 설정해야 합니다.

포털에 대한 자세한 내용은 사용자 가이드 또는 온라인 도움말에서 안티 스팸 장을 참고하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> portalregistrationconfig

Choose the operation you want to perform:

- REGISTRATION_ID - Set up the Registration ID.
[]> registration_id
Enter the new value of the Registration ID.
[]> registrationidexample1234

```

reboot

설명

어플라이언스를 다시 시작합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> reboot
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

repengstatus

설명

평판 엔진의 버전 정보를 요청합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> repengstatus
Component                Last Update                Version
Reputation Engine        28 Jan 2014 23:47 (GMT +00:00)  1
Reputation Engine Tools  28 Jan 2014 23:47 (GMT +00:00)  1
```

resume

설명

수신 및 전달을 다시 시작합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> resume
Receiving resumed for Listener 1.
Mail delivery resumed.
Mail delivery for individually suspended domains must be resumed individually.
```

resumedel

설명

전달을 다시 시작합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> resumedel
Currently suspended domains:
1. domain1.com
2. domain2.com
3. domain3.com
Enter one or more domains [comma-separated] to which you want to resume delivery.
[ALL]> domain1.com, domain2.com
Mail delivery resumed.
```

resumelistener

설명

리스너에서 수신을 다시 시작합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> resumelistener
Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Receiving resumed.
mail3.example.com>
```

회선

설명

이전 릴리스로 되돌립니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> revert
This command will revert the appliance to a previous version of AsyncOS.
WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all IronPort Spam Quarantine message and end-user safelist/blocklist data
Only the network settings will be preserved.
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passphrases unmasked)
- exported the IronPort Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty
Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots
again to the desired version.
  Available versions
  =====
  1. 9.1.0-019
Please select an AsyncOS version [1]:
Do you want to continue? [N]>
```

settime

설명

NTP 서버를 사용하지 않는 경우 **settime** 명령을 사용하면 수동으로 시간을 설정할 수 있습니다. 이 명령은 NTP를 중지하고 수동으로 시스템 시계를 설정할지 묻습니다. **MM/DD/YYYY HH:MM:SS** 형식으로 시간을 입력합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> settime
WARNING: Changes to system time will take place immediately
and do not require the user to run the commit command.
Current time 09/23/2001 21:03:53.
This machine is currently running NTP.
In order to manually set the time, NTP must be disabled.
Do you want to stop NTP and manually set the time? [N]> Y
Please enter the time in MM/DD/YYYY HH:MM:SS format.
[]> 09/23/2001 21:03:53
Time set to 09/23/2001 21:03:53.
```

settz

설명

현지 표준 시간대를 설정합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> settz
Current time zone: Etc/GMT
Current time zone version: 2010.02.0
Choose the operation you want to perform:
- SETUP - Set the local time zone.
[]> setup
Please choose your continent:
```

```

1. Africa
2. America
[ ... ]
11. GMT Offset
[2]> 2
Please choose your country:
1. Anguilla
[ ... ]
45. United States
46. Uruguay
47. Venezuela
48. Virgin Islands (British)
49. Virgin Islands (U.S.)
[45]> 45
Please choose your timezone:
1. Alaska Time (Anchorage)
2. Alaska Time - Alaska panhandle (Juneau)
[ ... ]
21. Pacific Time (Los_Angeles)
[21]> 21
Current time zone: America/Los_Angeles
Choose the operation you want to perform:
- SETUP - Set the local time zone.
[]>

```

shutdown

설명

전원을 끄기 위해 시스템을 종료합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail.example.com> shutdown
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System shutting down. Please wait while the queue is being closed...
Closing CLI connection.
The system will power off automatically.
Connection to mail.example.com closed.

```

smaconfig

- [설명, 125 페이지](#)
- [Usage\(사용\), 125 페이지](#)
- [예, 125 페이지](#)

설명

smaconfig 명령은 SMA 연결 파라미터 및 키를 추가, 삭제 또는 확인하는 데 사용됩니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

예

다음 예에서는 smaconfig 명령을 사용하여 사전 공유 키를 통해 SMA(Content Security Management Appliance)에 Email Security Appliance를 추가하고, SMA 연결 상세정보(호스트 이름 및 사용자 키)를 확인합니다.

```
mail.example.com> smaconfig
Choose the operation you want to perform:
- ADD - Add a new SMA Connection Parameter and Key.
[]> add

Enter the hostname of the system that you want to add.
[]> m380q03.ibqa

Enter the user key of the host m380q03.ibqa.
Press enter on a blank line to finish.

SSH2:dsa
10.76.71.107 ssh-dss
AAAAB3NzaC1kc3MAAACBAJCRYaVJgwSMItmLbt2xG5LVNKjFXpzW/vMRDQ3xclvJVpgYnQ1GfjL/zAbZC5pYz/jac405R9h
+J2jTzAjzZRgaBIalVviiLi0JkQQNhcFWEDjOhHwMTOKHh1+SVuqoR5xM0Y47jE/9SmEM6OXFSkAeTVXQg65c99FDGnNpveBWFAAAAAQD0dhuWPCD+
++xjLZr4yxLWFJ5AdQAAABiLaS
+VDYY38IosX/9czWGIcBl7cqDZUXWkwKF41OUfnoa42Q0VDBaoPiJ7gBhWVDHTo8rgz9PQRc10200k2ud7WASf/rLkbp9i26FWRK1yAAr7FvDoL/
l//5GtXbtMtqWYveo3oGqGS7dZc7MI/pMC5jGxDmTSM2SlyOEsS1xmQAAAIAY1ZiXC2ZeMhVWkgj8A8JHEPogT4hu7Mo3Yq+YkGsemK4L
+YF4k3t5DbGwirYvfxZCJSPD+E9mcnltIaQMFuB1W8Kiq+Cz/
Ikzm9U4MdIz48HOKS2S17YVG3xhYJjyyRpLHGDYRagANTjvOLRPF57xUvkdz5DCcJiXbWEhaZBHkg==

SMA host key was added successfully.

Choose the operation you want to perform:
- ADD - Add a new SMA Connection Parameter and Key.
- DELETE - Remove an existing SMA Connection Parameter and Key.
- PRINT - Display all SMA Parameters and Keys.

[]> print
1. Hostname: m380q03.ibqa Keys: SSH2:dsa10.76.71.107 ssh-dss
AAAAB3NzaC1kc3MAAACBAJCRYaVJgwSMItmLbt2xG5LVNKjFXpzW/vMRDQ3xclvJVpgYnQ1GfjL/zAbZC5pYz/jac405R9h
+J2jTzAjzZRgaBIalVviiLi0JkQQNhcFWEDjOhHwMTOKHh1+SVuqoR5xM0Y47jE/9SmEM6OXFSkAeTVXQg65c99FDGnNpveBWFAAAAAQD0dhuWPCD++
+xjLZr4yxLWFJ5AdQAAABiLaS
+VDYY38IosX/9czWGIcBl7cqDZUXWkwKF41OUfnoa42Q0VDBaoPiJ7gBhWVDHTo8rgz9PQRc10200k2ud7WASf/rLkbp9i26FWRK1yAAr7FvDoL/
l//5GtXbtMtqWYveo3oGqGS7dZc7MI/pMC5jGxDmTSM2SlyOEsS1xmQAAAIAY1ZiXC2ZeMhVWkgj8A8JHEPogT4hu7Mo3Yq+YkGsemK4L
+YF4k3t5DbGwirYvfxZCJSPD+E9mcnltIaQMFuB1W8Kiq+Cz/
Ikzm9U4MdIz48HOKS2S17YVG3xhYJjyyRpLHGDYRagANTjvOLRPF57xUvkdz5DCcJiXbWEhaZBHkg==
Choose the operation you want to perform:
- ADD - Add a new SMA Connection Parameter and Key.
- DELETE - Remove an existing SMA Connection Parameter and Key.
- PRINT - Display all SMA Parameters and Keys.
[]>
```

sshconfig

설명

SSH 서버 및 사용자 키 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 클러스터 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

- 예: SSH 서버 구성 수정, 126 페이지
- 예: 관리자 어카운트에 대해 새 공개 키 설치, 127 페이지
- 예: 영구 블랙리스트 또는 화이트리스트로 IP 주소 분류, 128 페이지

예: SSH 서버 구성 수정

다음 예에서는 SSH 서버 구성을 수정하는 방법을 보여 줍니다.

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
    rsal
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    arcfour256
    arcfour128
    aes128-cbc
    3des-cbc
    blowfish-cbc
    cast128-cbc
    aes192-cbc
    aes256-cbc
    arcfour
    rijndael-cbc@lysator.liu.se
MAC Methods:
    hmac-md5
    hmac-shal
    umac-64@openssh.com
    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-shal-96
    hmac-md5-96
Minimum Server Key Size:
    1024
KEX Algorithms:
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-shal
    diffie-hellman-group14-shal
    diffie-hellman-group1-shal
Choose the operation you want to perform:
```

```

- SETUP - Setup SSH server configuration settings
[ ]> setup
Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,
rijndael-cbc@lysator.liu.se]>
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96]>
Enter the Minimum Server Key Size do you want to use
[1024]>
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1]>
ssh server config settings:
Public Key Authentication Algorithms:
    rsa1
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    arcfour256
    arcfour128
    aes128-cbc
    3des-cbc
    blowfish-cbc
    cast128-cbc
    aes192-cbc
    aes256-cbc
    arcfour
    rijndael-cbc@lysator.liu.se
MAC Methods:
    hmac-md5
    hmac-sha1
    umac-64@openssh.com
    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-sha1-96
    hmac-md5-96
Minimum Server Key Size:
    1024
KEX Algorithms:
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-sha1
    diffie-hellman-group14-sha1
    diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[ ]>
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[ ]>

```

예: 관리자 어카운트에 대해 새 공개 키 설치

다음 예에서는 관리자 계정에 대해 새 공개 키가 설치됩니다.

```

mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings

```

예: 영구 블랙리스트 또는 화이트리스트로 IP 주소 분류

```

[ ]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[ ]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[ ]>

```

예: 영구 블랙리스트 또는 화이트리스트로 IP 주소 분류

어플라이언스 또는 ipblockd 서비스가 다시 시작되면 영구 블랙리스트 또는 화이트리스트로 분류한 IP 주소가 보존됩니다.



참고 AsyncOS 11.0.2 이상에서만 IP 주소를 영구 블랙리스트 또는 화이트리스트로 분류할 수 있습니다.

다음 예에서는 IP 주소를 영구 화이트리스트로 분류하는 방법을 보여 줍니다.

```

mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[ ]> access control

Choose the operation you want to perform:
- WHITELIST - Manage the persistent whitelist
- BLACKLIST - Manage the persistent blacklist
[ ]> whitelist

Choose the operation you want to perform:
- ADD - Add address(es)
- REMOVE - Remove address(es)
- PRINT - Print addresses
[ ]> add

Enter an IP address or a comma-separated list of addresses.
Addresses already in the Whitelist will be ignored.
[ ]> 10.8.85.77

```

The addresses were successfully added to the Whitelist

다음 예에서는 IP 주소를 영구 블랙리스트로 분류하는 방법을 보여 줍니다.

```

mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[ ]> access control

Choose the operation you want to perform:
- WHITELIST - Manage the persistent whitelist
- BLACKLIST - Manage the persistent blacklist
[ ]> blacklist

```

```

Choose the operation you want to perform:
- ADD - Add address(es)
- REMOVE - Remove address(es)
- PRINT - Print addresses
[]> add

Enter an IP address or a comma-separated list of addresses.
Addresses already in the Whitelist will be ignored.
[]> 10.8.85.77

The addresses were successfully added to the blacklist

```

status

설명

시스템 상태를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> status

Status as of: Thu Oct 21 14:33:27 2004 PDT
Up since: Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset: Never
System status: Online
Oldest Message: 4 weeks 46 mins 53 secs
Feature - McAfee: 161 days
[...]
Feature - Outbreak Filters: 161 days
Counters:
Receiving
  Messages Received 62,049,822 290,920 62,049,822
  Recipients Received 62,049,823 290,920 62,049,823
Rejection
  Rejected Recipients 3,949,663 11,921 3,949,663
  Dropped Messages 11,606,037 219 11,606,037
Queue
  Soft Bounced Events 2,334,552 13,598 2,334,552
Completion
  Completed Recipients 50,441,741 332,625 50,441,741
Current IDs
  Message ID (MID) 99524480
  Injection Conn. ID (ICID) 51180368
  Delivery Conn. ID (DCID) 17550674
Gauges:
Connections
  Current Inbound Conn. 0
  Current Outbound Conn. 14

```

```

Queue
  Active Recipients                1
  Messages In Work Queue          0
  Kilobytes Used                   92
  Kilobytes Free                   8,388,516
Quarantine
  Messages In Quarantine
    Policy, Virus and Outbreak    0
  Kilobytes In Quarantine
    Policy, Virus and Outbreak    0

```

supportrequest

설명

Cisco 고객 지원에 메시지를 보냅니다. 이 명령을 사용하려면 어플라이언스에서 인터넷에 메일을 보낼 수 있어야 합니다. 장애 처리가 자동으로 생성됩니다. 또는 지원 요청을 기존 장애 처리와 연결할 수 있습니다.

어플라이언스에서 직접 Cisco 기술 지원에 액세스하려면 Cisco.com 사용자 ID가 이 어플라이언스의 서비스 계약과 연결되어 있어야 합니다. 현재 Cisco.com 프로파일과 연결되어 있는 서비스 계약의 목록을 보려면 Cisco.com 프로파일 관리자(<https://sso.cisco.com/auth/forms/CDClogin.html>)를 방문하십시오. Cisco.com 사용자 ID가 없을 경우 등록하여 생성합니다. 계정 등록에 대한 자세한 내용은 해당 릴리스의 온라인 도움말 또는 사용 설명서를 참조하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 기존 지원 티켓과 무관한 지원 요청을 보여줍니다.

```

mail.example.com> supportrequest
Please Note:
If you have an urgent issue, please call one of our worldwide Support Centers
(www.cisco.com/support). Use this command to open a technical support request
for issues that are not urgent, such as:
- Request for information.
- Problem for which you have a work-around, but would like an alternative
solution.
Do you want to send the support request to supportrequest@mail.ga?
[Y]>
Do you want to send the support request to additional recipient(s)?
[N]>
Is this support request associated with an existing support ticket?
[N]>
Please select a technology related to this support request:
1. Security - Email and Web
2. Security - Management

```

```

[1]> 1
Please select a subtechnology related to this support request:
1. Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - Misclassified
Messages
2. Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - SBRS
3. Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - Other
4. Email Security Appliance - Virtual
[1]> 3
Please select the problem category:
1. Upgrade
2. Operate
3. Configure
4. Install
[1]> 3
Please select a problem sub-category:
1. Error Messages, Logs, Debugs
2. Software Failure
3. Interoperability
4. Configuration Assistance
5. Install, Uninstall or Upgrade
6. Hardware Failure
7. Licensing
8. Data Corruption
9. Software Selection/Download Assistance
10. Passphrase Recovery
[1]> 5
Please enter a subject line for this support request:
[]> <Subject line for support request>
Please enter a description of your issue, providing as much detail as possible
to aid in diagnosis:
[]> <Description of issue>
It is important to associate all your service contracts with your Cisco.com profile (CCO
ID) in order for you to receive complete
access to support and services from Cisco. Please follow the URLs below to associate your
contract coverage on your Cisco.com profile.
If you do not have a CCO ID, please follow
the URL below to create a CCO ID.
How to create a CCO ID:
https://tools.cisco.com/RPF/register/register.do
How to associate your CCO ID with contract:
https://tools.cisco.com/RPFA/profile/profile_management.do
Frequently Asked Question:
http://www.cisco.com/web/ordering/cs_info/faqs/index.html
Select the CCOID
1. New CCOID
[1]>
Please enter the CCOID of the contact person :
[]> your name
The CCO ID may contain alphabets, numbers and '@', '.', '-' and '_' symbols.
Please enter the CCOID of the contact person :
[]> me@example.com
Please enter the name of the contact person :
[]> yourname
Please enter your email address:
[]> me@example.com
Please enter the contract ID:
[]> 1234
Please enter any additional contact information (e.g. phone number):
[]>
Please wait while configuration information is generated...
Do you want to print the support request to the screen?
[N]>

```

supportrequeststatus

설명

Cisco TAC 지원을 요청하기 위해 지원 요청 키워드 버전 정보를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> supportrequeststatus
Component          Version    Last Updated
Support Request    1.0       Never updated
```

supportrequestupdate

설명

Cisco TAC 지원을 요청하기 위해 지원 요청 키워드의 수동 업데이트를 요청합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> supportrequestupdate
Requesting update of Support Request Keywords.
```

suspend

설명

수신 및 전달을 일시 중단합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> suspend
Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
Waiting for listeners to exit...
Receiving suspended for Listener 1.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com>
```

suspenddel

설명

전달을 일시 중단합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> suspenddel
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Enter one or more domains [comma-separated] to which you want to suspend delivery.
[ALL]> domain1.com, domain2.com, domain3.com
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

suspendlistener

설명

수신을 일시 중단합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> suspendlistener
Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

tcpservices

설명

프로세스에서 여는 파일에 대한 정보를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.cisco.com> tcpservices
System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon
Feature Processes
  euq_webui    - GUI for ISQ
  gui          - GUI process
  hermes       - MGA mail server
  postgres    - Process for storing and querying quarantine data
  splunkd     - Processes for storing and querying Email Tracking data
COMMAND      USER      TYPE  NODE  NAME
interface    root      IPv4  TCP   127.0.0.1:53
postgres     pgsqldb  IPv4  TCP   127.0.0.1:5432
qabackdoo    root      IPv4  TCP   *:8123
ftpd.main    root      IPv4  TCP   10.1.1.0:21
euq_webui    root      IPv4  TCP   10.1.1.0:83
euq_webui    root      IPv6  TCP   [2001:db8::]:83
gui          root      IPv4  TCP   172.29.181.70:80
gui          root      IPv4  TCP   10.1.1.0:80
```

```

gui          root          IPv6 TCP    [2001:db8::]:80
gui          root          IPv4 TCP    172.29.181.70:443
gui          root          IPv4 TCP    10.1.1.0:443
gui          root          IPv6 TCP    [2001:db8::]:443
ginetd      root          IPv4 TCP    172.29.181.70:22
ginetd      root          IPv4 TCP    10.1.1.0:22
ginetd      root          IPv6 TCP    [2001:db8::]:22
ginetd      root          IPv4 TCP    10.1.1.0:2222
ginetd      root          IPv6 TCP    [2001:db8::]:2222
hermes      root          IPv4 TCP    172.29.181.70:25
splunkd     root          IPv4 TCP    127.0.0.1:8089
splunkd     root          IPv4 TCP    127.0.0.1:9997
api_serve  root          IPv4 TCP    10.1.1.0:6080
api_serve  root          IPv6 TCP    [2001:db8::]:6080
api_serve  root          IPv4 TCP    10.1.1.0:6443
api_serve  root          IPv6 TCP    [2001:db8::]:6443
java       root          IPv6 TCP    [::127.0.0.1]:9999

```

techsupport

설명

Cisco TAC의 시스템 액세스를 허용합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> techsupport
Service Access currently disabled.
Serial Number: XXXXXXXXXXXX-XXXXXXX
Choose the operation you want to perform:
- SSHACCESS - Allow a Cisco IronPort Customer Support representative to remotely access
your system, without establishing a tunnel.
- TUNNEL - Allow a Cisco IronPort Customer Support representative to remotely access your
system, and establish a secure tunnel
              for communication.
- STATUS - Display the current techsupport status.
[ ]> sshaccess
A random seed string is required for this operation
1. Generate a random string to initialize secure communication (recommended)
2. Enter a random string
[1]> 1
Are you sure you want to enable service access? [N]> y
Service access has been ENABLED. Please provide the string:
QT22-JQZF-YAQL-TL8L-8@2L-95
to your Cisco IronPort Customer Support representative.
Service Access currently ENABLED (0 current service logins).
Tunnel option is not active.
Serial Number: XXXXXXXXXXXX-XXXXXXX
Choose the operation you want to perform:
- DISABLE - Prevent customer service representatives from remotely accessing your system.

```

```
- STATUS - Display the current techsupport status.
[]>
```

tlsverify

설명

필요에 따라 아웃바운드 TLS 연결을 설정하고 목적지 도메인과 관련된 어떤 TLS 연결 문제도 디버깅합니다. 연결을 생성하려면 확인 대상이 될 도메인 및 목적지 호스트를 지정합니다. AsyncOS에서는 Required (Verify) TLS(필수(확인) TLS) 설정에 따라 TLS 연결을 확인합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

tlsverify 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있으며, 이를 통해 지정된 호스트 이름과의 TLS 연결을 확인합니다.

```
tlsverify <domain> <hostname>[:<port>]
```

예

```
mail3.example.com> tlsverify
Enter the TLS domain to verify against:
[]> example.com
Enter the destination host to connect to. Append the port (example.com:26) if you are not
connecting on port 25:
[example.com]> mxe.example.com:25
Connecting to 1.1.1.1 on port 25.
Connected to 1.1.1.1 from interface 10.10.10.10.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher RC4-SHA.
Verifying peer certificate.
Verifying certificate common name mxe.example.com.
TLS certificate match mxe.example.com
TLS certificate verified.
TLS connection to 1.1.1.1 succeeded.
TLS successfully connected to mxe.example.com.
TLS verification completed.
```

trace

설명

시스템을 지나는 메시지의 플로우를 추적합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> trace
Enter the source IP
[]> 192.168.1.1
Enter the fully qualified domain name of the source IP
[]> example.com
Select the listener to trace behavior on:
1. InboundMail
2. OutboundMail
[1]> 1
Fetching default SenderBase values...
Enter the SenderBase Org ID of the source IP. The actual ID is N/A.
[N/A]>
Enter the SenderBase Reputation Score of the source IP. The actual score is N/A.
[N/A]>
Enter the Envelope Sender address:
[]> pretend.sender@example.net
Enter the Envelope Recipient addresses. Separate multiple addresses by commas.
[]> admin@example.com
Load message from disk? [Y]> n
Enter or paste the message body here. Enter '.' on a blank line to end.
Subject: Hello
This is a test message.
.
HAT matched on unnamed sender group, host ALL
- Applying $ACCEPTED policy (ACCEPT behavior).
- Maximum Message Size: 100M (Default)
- Maximum Number Of Connections From A Single IP: 1000 (Default)
- Maximum Number Of Messages Per Connection: 1,000 (Default)
- Maximum Number Of Recipients Per Message: 1,000 (Default)
- Maximum Recipients Per Hour: 100 (Default)
- Use SenderBase For Flow Control: Yes (Default)
- Spam Detection Enabled: Yes (Default)
- Virus Detection Enabled: Yes (Default)
- Allow TLS Connections: No (Default)
Processing MAIL FROM:
- Default Domain Processing: No Change
Processing Recipient List:
Processing admin@ironport.com
- Default Domain Processing: No Change
- Domain Map: No Change
- RAT matched on admin@ironport.com, behavior = ACCEPT
- Alias expansion: No Change
Message Processing:
- No Virtual Gateway(tm) Assigned
- No Bounce Profile Assigned
Domain Masquerading/LDAP Processing:
- No Changes.
Processing filter 'always_deliver':
Evaluating Rule: rcpt-to == "@mail.qa"
Result = False
Evaluating Rule: rcpt-to == "ironport.com"
```

```

    Result = True
Evaluating Rule:   OR
    Result = True
Executing Action:  deliver()
Footer Stamping:
- Not Performed
Inbound Recipient Policy Processing: (matched on Management Upgrade policy)
Message going to: admin@ironport.com
AntiSpam Evaluation:
- Not Spam
AntiVirus Evaluation:
- Message Clean.
- Elapsed Time = '0.000 sec'
Outbreak Filter Evaluation:
- No threat detected
Message Enqueued for Delivery
Would you like to see the resulting message? [Y]> y
Final text for messages matched on policy Management Upgrade
Final Envelope Sender: pretend.sender@example.doma
Final Recipients:
- admin@ironport.com
Final Message Content:
Received: from remotehost.example.com (HELO TEST) (1.2.3.4)
    by stacy.qa with TEST; 19 Oct 2004 00:54:48 -0700
Message-Id: <3i93q9$@Management>
X-IronPort-AV: i="3.86,81,1096873200";
    d="scan'208"; a="0:sNHT0"
Subject: hello
This is a test message.
Run through another debug session? [N]>

```



참고 trace를 사용할 때 메시지의 헤더와 본문을 모두 CLI에 붙여 넣어야 합니다.

trackingconfig

설명

추적 시스템을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail.example.com> trackingconfig
Message Tracking service status: Message Tracking is enabled.
Choose the operation you want to perform:
- SETUP - Enable Message Tracking for this appliance.
[]> setup
Would you like to use the Message Tracking Service? [Y]>

```

```

Do you want to use Centralized Message Tracking for this appliance? [N]>
Would you like to track rejected connections? [N]>
Message Tracking service status: Local Message Tracking is enabled.
Rejected connections are currently not being tracked.
Choose the operation you want to perform:
- SETUP - Enable Message Tracking for this appliance.
[]>

```

tzupdate

설명

표준 시간대 규칙을 업데이트합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

배치 형식

tzupdate 명령의 배치 형식은 변경 사항이 없더라도 모든 표준 시간대 규칙을 강제적으로 업데이트합니다.

```
tzupdate [force]
```

예

```
mail.example.com> tzupdate
Requesting update of Timezone Rules
```

updateconfig

설명

시스템 업데이트 매개변수를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

- 업데이트 서버에서 업데이트를 다운로드하도록 어플라이언스 구성, 140 페이지
- 업데이트 서버 인증서의 유효성을 확인하도록 어플라이언스 구성, 142 페이지
- 어플라이언스에서 프록시 서버 통신을 신뢰하도록 구성, 143 페이지

업데이트 서버에서 업데이트를 다운로드하도록 어플라이언스 구성

다음 예에서는 `updateconfig` 명령을 사용하여 어플라이언스가 Cisco 서버에서 업데이트 이미지를 다운로드하고 로컬 서버에서 사용 가능 AsyncOS 업그레이드의 목록을 다운로드하도록 구성합니다.

```
mail.example.com> updateconfig
Service (images):
-----
Feature Key updates
Timezone rules
Enrollment Client Updates
Support Request updates
Cisco IronPort AsyncOS upgrades
Service (list):
-----
Update URL:
http://downloads.ironport.com/asyncos
Cisco IronPort Servers
Cisco IronPort Servers
Cisco IronPort Servers
Cisco IronPort Servers
Update URL:
-----
Timezone rules
Enrollment Client Updates
Support Request updates
Service (list):
-----
Update URL:
Cisco IronPort Servers
Cisco IronPort Servers
Cisco IronPort Servers
Update URL:
-----
Cisco IronPort AsyncOS upgrades
Update interval: 5m
Alert Interval for Disabled Automatic Engine Updates: 30d
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[ ]> setup
For the following services, please select where the system will download updates from:
Service (images):
-----
Update URL:
http://downloads.ironport.com/asyncos
1. Use Cisco IronPort update servers (http://downloads.ironport.com)
2. Use own server
[1]>
For the following services, please select where the system will download updates from
(images):
Service (images):
-----
Update URL:
Timezone rules
Enrollment Client Updates
Support Request updates
Cisco IronPort Servers
Cisco IronPort Servers
Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own server
[1]>
For the following services, please select where the system will download updates from
(images):
Service (images):
-----
Update URL:
Cisco IronPort AsyncOS upgrades
Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own server
```



```

[1]>
For the following services, please select where the system will download the list of available
updates from:
Service (list):                                Update URL:
-----
Timezone rules                                Cisco IronPort Servers
Enrollment Client Updates                    Cisco IronPort Servers
Support Request updates                      Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own update list
[1]>
For the following services, please select where the system will download the list of available
updates from:
Service (list):                                Update URL:
-----
Cisco IronPort AsyncOS upgrades             Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own update list
[1]>
Enter the time interval between checks for new:
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
Use a trailing 's' for seconds, 'm' for minutes or 'h' for hours. The minimum
valid update time is 30s or enter '0' to disable automatic updates (manual
updates will still be available for individual services).
[5m]>
When initiating a connection to the update server the originating IP interface
is chosen automatically. If you want to choose a specific interface, please
specify it now.
1. Auto
2. Management (10.76.69.149/24: vm30esa0086.ibqa)
[1]>
Do you want to set up a proxy server for HTTP updates for ALL of the following
services:
- Feature Key updates
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
- Cisco IronPort AsyncOS upgrades
[N]>
Do you want to set up an HTTPS proxy server for HTTPS updates for ALL of the following
services:
- Feature Key updates
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
- Cisco IronPort AsyncOS upgrades
- SenderBase Network Participation sharing
[N]>
Service (images):                                Update URL:
-----
Feature Key updates                            http://downloads.ironport.com/asynco
Timezone rules                                Cisco IronPort Servers
Enrollment Client Updates                    Cisco IronPort Servers
Support Request updates                      Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades             Cisco IronPort Servers
Service (list):                                Update URL:
-----
Timezone rules                                Cisco IronPort Servers
Enrollment Client Updates                    Cisco IronPort Servers
Support Request updates                      Cisco IronPort Servers
Service (list):                                Update URL:
-----

```

```

Cisco IronPort AsyncOS upgrades                               Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>

```

업데이트 서버 인증서의 유효성을 확인하도록 어플라이언스 구성

이 옵션을 구성할 경우 어플라이언스가 Cisco 업데이트 서버와 통신할 때마다 업데이트 서버 인증서의 유효성이 확인됩니다. 이 확인을 통과하지 못할 경우 업데이트가 다운로드되지 않으며 세부 사항이 업데이트 로그에 기록됩니다. 다음 예에서는 이 옵션을 구성하는 방법을 보여줍니다.

```

mail.example.com> updateconfig
Service (images):                                           Update URL:
-----
Feature Key updates                                       http://downloads.ironport.com/asyncos
Timezone rules                                           Cisco IronPort Servers
Enrollment Client Updates                               Cisco IronPort Servers
Support Request updates                                  Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                         Cisco IronPort Servers
Service (list):                                          Update URL:
-----
Timezone rules                                           Cisco IronPort Servers
Enrollment Client Updates                               Cisco IronPort Servers
Support Request updates                                  Cisco IronPort Servers
Service (list):                                          Update URL:
-----
Cisco IronPort AsyncOS upgrades                         Cisco IronPort Servers
Update interval: 5m
Alert Interval for Disabled Automatic Engine Updates: 30d
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                           Update URL:
-----
Feature Key updates                                       http://downloads.ironport.com/asyncos
Timezone rules                                           Cisco IronPort Servers
Enrollment Client Updates                               Cisco IronPort Servers
Support Request updates                                  Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                         Cisco IronPort Servers
Service (list):                                          Update URL:
-----
Timezone rules                                           Cisco IronPort Servers
Enrollment Client Updates                               Cisco IronPort Servers
Support Request updates                                  Cisco IronPort Servers
Service (list):                                          Update URL:
-----
Cisco IronPort AsyncOS upgrades                         Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:

```

```
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

어플라이언스에서 프록시 서버 통신을 신뢰하도록 구성

투명하지 않은 프록시 서버를 사용 중인 경우, 프록시 인증서 서명에 사용된 CA 인증서를 어플라이언스에 추가할 수 있습니다. 그렇게 함으로써 어플라이언스는 프록시 서버 통신을 신뢰합니다. 다음 예에서는 이 옵션을 구성하는 방법을 보여줍니다.

```
...
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
[]> add
Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
Paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MMIICiDCCAFgGawIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhmMCSU4x
DDAKBgNVBAGTA0tBUjENM.....
-----END CERTIFICATE-----
.
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

updatenow

설명

모든 시스템 서비스 구성 요소에 대한 업데이트를 요청합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

updatenow 명령의 배치 형식은 변경 사항이 없더라도 어플라이언스의 모든 구성 요소를 업데이트하는 데 사용할 수 있습니다.

```
updatenow [force]
```

예

예

```
mail3.example.com> updatenow
Success - All component updates requested
```

버전

설명

시스템 버전 정보를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> version
Current Version
=====
Product: Cisco C100V Email Security Virtual Appliance
Model: C100V
Version: 9.1.0-019
Build Date: 2015-02-17
Install Date: 2015-02-19 05:17:56
Serial #: 421C73B18CFB05784A83-B03A99E71ED8
BIOS: 6.00
CPUs: 2 expected, 2 allocated
Memory: 6144 MB expected, 6144 MB allocated
RAID: NA
RAID Status: Unknown
RAID Type: NA
BMC: NA
```

wipedata

설명

디스크의 코어 파일을 지우고 마지막 코어덤프 작업의 상태를 확인하려면 **wipedata** 명령을 사용합니다.



참고 데이터의 크기에 따라 지우기 작업에 다소 시간이 걸리고 작업 완료까지 시스템 성능에 영향을 미칠 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> wipedata
Wiping data may take a while and can affect system performance till it completes.
Choose the operation you want to perform:
- STATUS - Display status of last command run
- COREDUMP - Wipe core files on disk
[]> coredump
wipedata: In progress
mail.example.com> wipedata
Wiping data may take a while and can affect system performance till it completes.
Choose the operation you want to perform:
- STATUS - Display status of last command run
- COREDUMP - Wipe core files on disk
[]> status
Last wipedata status: Successful
```

upgrade

설명

upgrade CLI 명령은 사용 가능한 업그레이드 목록을 표시하고 AsyncOS 시스템을 사용자가 지정한 버전으로 업그레이드합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> upgrade
Upgrades available:
1. AsyncOS (**DON'T TOUCH**) 4.0.8 upgrade, 2005-05-09 Build 900
2. AsyncOS 4.0.8 upgrade, 2005-08-12 Build 030
.....
45. SenderBase Network Participation Patch
[45]>
Performing an upgrade will require a reboot of the system after the upgrade is applied.
Do you wish to proceed with the upgrade? [Y]> Y
```

콘텐츠 스캔

- [contentscannerstatus, 146 페이지](#)
- [contentscannerudpate, 146 페이지](#)

contentscannerstatus

콘텐츠 스캐닝 엔진 버전 정보를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> contentscannerstatus
Component          Version          Last Updated
Content Scanner Tools 11.2.1884.970097 Never updated
```

contentscannerudpate

콘텐츠 스캐닝 엔진의 수동 업데이트를 요청합니다. 'force' 파라미터를 사용하면 탐지된 변경 사항이 없는 경우에도 업데이트가 수행됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> contentscannerupdate force
Requesting forced update for Content Scanner.
```

LDAP

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [ldapconfig, 147 페이지](#)

- [ldapflush, 151 페이지](#)
- [ldaptest, 151 페이지](#)
- [sievechar, 152 페이지](#)

ldapconfig

설명

LDAP 서버를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예 - 새 LDAP 서버 프로필 생성

다음 예에서는 `ldapconfig` 명령을 사용하여 어플라이언스에서 바인딩할 수 있는 LDAP 서버를 정의합니다. 또한 수신자 수락(`ldapaccept` 하위 명령), 라우팅(`ldaprouting` 하위 명령), masquerading(`masquerade` 하위 명령), 스팸 격리를 위한 엔드 유저 인증(`isqauth subcommand`), 스팸 알림을 위한 별칭 통합(`isqalias` 하위 명령)을 위한 쿼리를 구성합니다.

먼저 `mldapserver.example.com` LDAP 서버에 "PublicLDAP"라는 별칭이 지정됩니다. Queries are directed to port 3268 (the default). 검색 기준으로 `example.com`이 정의되고(`dc=example,dc=com`) 수신자 수락, 메일 리라우팅, 가장을 위한 쿼리가 정의됩니다. 이 예의 쿼리는 만료된 Internet Draft *draft-lachman-laser-ldap-mail-routing-xx.txt* ("Laser spec"이라고도 함)에 정의된 `inetLocalMailRecipient` 보조 개체 클래스를 사용하는 OpenLDAP 디렉터리 구성과 유사합니다. 이 초안의 버전 하나가 OpenLDAP 소스 배포판과 함께 제공됩니다. 이 예에서는 메일 리라우팅 쿼리에서 쿼리된 수신자에 사용할 대체 메일 호스트가 `mailForwardingAddress`입니다. 쿼리 이름은 대/소문자를 구분하며 정확히 매치해야 알맞은 결과가 반환됩니다.

```
mail3.example.com> ldapconfig
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]> new
Please create a name for this server configuration (Ex: "PublicLDAP"):
[]> PublicLDAP
Please enter the hostname:
[]> myldapserver.example.com
Use SSL to connect to the LDAP server? [N]> n
Select the authentication method to use for this server configuration:
1. Anonymous
2. Passphrase based
[1]> 2
Please enter the bind username:
[cn=Anonymous]>
Please enter the bind passphrase:
```

```

[ ]>
Connect to LDAP server to validate setting? [Y]
Connecting to the LDAP server, please wait...
Select the server type to use for this server configuration:
1. Active Directory
2. OpenLDAP
3. Unknown or Other
[3]> 1

Please enter the port number:
[3268]> 3268
Please enter the base:
[dc=example,dc=com]> dc=example,dc=com
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- TEST - Test the server configuration.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- CERTAUTH - Configure certificate authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[ ]> ldapaccept
Please create a name for this query:
[PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept
Enter the LDAP query string:
[(proxyAddresses=smtp:{a})]> (proxyAddresses=smtp:{a})
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[ ]> ldaprouting
Please create a name for this query:
[PublicLDAP.routing]> PublicLDAP.routing
Enter the LDAP query string:
[(mailLocalAddress={a})]> (mailLocalAddress={a})
The query requires one of the attributes below. Please make a selection.
  [1] Configure MAILROUTINGADDRESS only - Rewrite the Envelope Recipient (and
leave MAILHOST unconfigured)?
  [2] Configure MAILHOST only - Send the messages to an alternate mail host
(and leave MAILROUTINGADDRESS unconfigured)?
  [3] Configure both attributes

```



```

[ ]> 1
Enter the attribute which contains the full rfc822 email address for the
recipients.
[mailRoutingAddress]> mailRoutingAddress
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[ ]> masquerade
Please create a name for this query:
[PublicLDAP.masquerade]> PublicLDAP.masquerade
Enter the LDAP query string:
[(mailRoutingAddress={a})]> (mailRoutingAddress={a})
Enter the attribute which contains the externally visible full rfc822 email address.
[ ]> mailLocalAddress
Do you want the results of the returned attribute to replace the entire friendly portion
of the original recipient? [N]> n
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
MASQUERADE: PublicLDAP.masquerade
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[ ]> isqauth
Please create a name for this query:
[PublicLDAP.isqauth]> PublicLDAP.isqauth
Enter the LDAP query string:
[(sAMAccountName={u})]> (sAMAccountName={u})
Enter the list of email attributes.
[ ]> mail,proxyAddresses
Do you want to activate this query? [Y]> y
Do you want to test this query? [Y]> y
User identity to use in query:
[ ]> admin@example.com
Passphrase to use in query:
[ ]> passphrase
LDAP query test results:

```

```

LDAP Server: myldapserver.example.com
Query: PublicLDAP.isqauth
User: admin@example.com
Action: match positive
LDAP query test finished.
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
MASQUERADE: PublicLDAP.masquerade
ISQAUTH: PublicLDAP.isqauth [active]
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]>
Current LDAP server configurations:
1. PublicLDAP: (myldapserver.example.com:3268)
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
- EDIT - Modify a server configuration.
- DELETE - Remove a server configuration.
[]>

```

예 - 전역 설정 구성

다음 예에서는 TLS 연결용 인증서를 포함하여 LDAP 전역 설정이 구성됩니다.

```

mail3.example.com> ldapconfig
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]> setup
Choose the IP interface for LDAP traffic.
1. Auto
2. Management (10.92.145.175/24: esx16-esa01.qa)
[1]> 1
LDAP will determine the interface automatically.
Should group queries that fail to complete be silently treated as having
negative results? [Y]>
Validate LDAP server certificate? [Y]>
The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure.
1. partner.com
2. Demo
Please choose the certificate to apply:
[1]> 1
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.

```

```
- SETUP - Configure LDAP options.
[]>
```

ldapflush

설명

캐싱된 LDAP 결과를 플러시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> ldapflush
Are you sure you want to flush any cached LDAP results? [N]> y
Flushing cache
mail3.example.com>
```

ldaptest

설명

단일 LDAP 쿼리 테스트를 수행합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 `ldaptest` 명령을 사용하여 구성된 LDAP 서버 컨피그레이션에 대한 유일한 수신자 수락 쿼리를 테스트합니다. 수신자 주소 “`admin@example.com`”이 테스트를 통과하지만, 수신자 주소 “`bogus@example.com`”은 통과하지 못합니다.

```
mail3.example.com> ldaptest
Select which LDAP query to test:
1. PublicLDAP.ldapaccep
[1]> 1
Address to use in query:
[]> admin@example.com
LDAP query test results:
```

```

        Query: PublicLDAP.ldapaccept
        Argument: admin@example.com
        Action: pass
LDAP query test finished.
mail3.example.com> ldaptest
Select which LDAP query to test:
1. PublicLDAP.ldapaccep
[1]> 1
Address to use in query:
[]> bogus@example.com
LDAP query test results:
  Query: PublicLDAP.ldapaccept
  Argument: bogus@example.com
  Action: drop or bounce (depending on listener settings)
  Reason: no matching LDAP record was found
LDAP query test finished.
mail3.example.com>

```

sievechar

설명

RFC 3598에 따른 Sieve 이메일 필터링에 쓰이는 문자를 설정하거나 비활성화합니다. Sieve 문자는 LDAP Accept 및 LDAP Reroute 쿼리에서만 인식됩니다. 시스템의 다른 부분에서는 전체 이메일 주소를 사용합니다.

허용되는 문자는 `-_=#`입니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 `sievechar` 명령을 사용하여 `+`를 Accept 및 LDAP Reroute 쿼리에서 인식되는 Sieve 문자로 정의합니다.

```

mail3.example.com> sievechar
Sieve Email Filtering is currently disabled.
Choose the operation you want to perform:
- SETUP - Set the separator character.
[]> setup
Enter the Sieve Filter Character, or a space to disable Sieve Filtering.
[]> +
Sieve Email Filter is enabled, using the '+' character as separator.
This applies only to LDAP Accept and LDAP Reroute Queries.
Choose the operation you want to perform:
- SETUP - Set the separator character.
[]>

```

메일 전달 컨피그레이션/모니터링

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [addresslistconfig](#), 153 페이지
- [aliasconfig](#), 155 페이지
- [archivemessage](#), 157 페이지
- [altsrchoost](#), 158 페이지
- [bounceconfig](#), 159 페이지
- [bouncerecipients](#), 162 페이지
- [bvconfig](#), 163 페이지
- [deleterecipients](#), 164 페이지
- [deliveryconfig](#), 166 페이지
- [delivernow](#), 166 페이지
- [destconfig](#), 167 페이지
- [hostrate](#), 175 페이지
- [hoststatus](#), 175 페이지
- [imageanalysisconfig](#), 177 페이지
- [oldmessage](#), 178 페이지
- [rate](#), 178 페이지
- [redirectrecipients](#), 179 페이지
- [resetcounters](#), 180 페이지
- [removemessage](#), 180 페이지
- [showmessage](#), 181 페이지
- [showrecipients](#), 181 페이지
- [status](#), 129 페이지
- [tophosts](#), 184 페이지
- [topin](#), 184 페이지
- [unsubscribe](#), 185 페이지
- [workqueue](#), 186 페이지

addresslistconfig

설명

주소 목록을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

`addresslistconfig` 명령의 배치 형식은 새 주소 목록을 생성하고 기존 주소 목록을 수정하고 주소 목록을 나열하여 인쇄하고 주소 목록을 삭제하고 한 주소 목록 내에서 충돌하는 주소를 찾는 데 사용할 수 있습니다.

- 새 주소 목록 추가:

```
addresslistconfig new <name> --descr=<description> --addresses=<address1,address2,...>
```

- 기존 주소 목록 수정:

```
addresslistconfig edit <name> --name=<new-name> --descr=<description>
--addresses=<address1,address2,...>
```

- 주소 목록 삭제:

```
addresslistconfig delete <name>
```

- 주소 목록 나열 및 인쇄:

```
addresslistconfig print <name>
```

- 주소 목록 내에서 충돌하는 주소 찾기:

```
addresslistconfig conflicts <name>
```

예

```
mail1.example.com> addresslistconfig

No address lists configured.

Choose the operation you want to perform:
- NEW - Create a new address list.
[ ]> new

Enter a name for the address list:
> add-list1

Enter a description for the address list:
> This is a sample address list

Enter the type of list:
1. Full Email Addresses only
2. Domains only
3. IP Addresses only
4. All of the above
Enter the type of the address list:
[4]> 1

Enter a comma separated list of addresses:
(e.g.: user@example.com)
> user1@example.com, user2@example.com
```

```
Address list "add-list1" added.

Choose the operation you want to perform:
- NEW - Create a new address list.
- EDIT - Modify an address list.
- DELETE - Remove an address list.
- PRINT - Display the contents of an address list.
- CONFLICTS - Find conflicting entries within an address list.
[]>
```

aliasconfig

설명

이메일 별칭을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

aliasconfig 명령의 배치 형식은 새 별칭 테이블을 추가하고 기존 테이블을 수정하고 이메일 별칭 목록을 인쇄하고 별칭 목록의 가져오기/내보내기를 수행하는 데 사용할 수 있습니다. 배치 명령을 실행하려면 다음 형식의 aliasconfig 명령을 아래에 나열된 변수와 함께 사용합니다.

- 새 이메일 별칭 추가:

```
aliasconfig new <domain> <alias> [email_address1] [email_address2] ...
```



참고 'aliasconfig new' 명령을 존재하지 않는 도메인과 함께 사용할 경우 해당 도메인이 생성됩니다.

- 기존 이메일 별칭 수정:

```
aliasconfig edit <domain> <alias> <email_address1> [email_address2] ...
```

- 이메일 별칭 표시:

```
aliasconfig print
```

- 로컬 별칭 목록 가져오기:

```
aliasconfig import <filename>
```

- 어플라이언스에서 별칭 목록 내보내기:

```
aliasconfig export <filename>
```

예

```
mail3.example.com> aliasconfig
Enter address(es) for "customercare".
Separate multiple addresses with commas.
[ ]> bob@example.com, frank@example.com, sally@example.com
Adding alias customercare: bob@example.com,frank@example.com,sally@example.com
Do you want to add another alias? [N]> n
There are currently 1 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[ ]> new
How do you want your aliases to apply?
1. Globally
2. Add a new domain context
3. example.com
[1]> 1
Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
- "user@domain" - This email address.
- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.
[ ]> admin
Enter address(es) for "admin".
Separate multiple addresses with commas.
[ ]> administrator@example.com
Adding alias admin: administrator@example.com
Do you want to add another alias? [N]> n
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[ ]> print
admin: administrator@example.com
[ example.com ]
```



```

customercare: bob@example.com, frank@example.com, sally@example.com
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]>

```

표 6: 별칭 구성을 위한 인수

인수	설명
<domain>	별칭이 적용되는 도메인 컨텍스트. 'Global'은 전역 도메인 컨텍스트를 지정합니다.
<alias>	구성할 별칭의 이름 전역 도메인 컨텍스트에서 허용되는 별칭: 'user@domain' — 해당 이메일 주소 'user' — 임의 도메인의 해당 사용자 '@domain' — 해당 도메인의 모든 사용자 '@.partialdomain' — 해당 도메인 또는 그 모든 하위 도메인의 모든 사용자 특정 도메인 컨텍스트에서 허용되는 별칭: 'user' — 해당 도메인 컨텍스트의 해당 사용자 'user@domain' — 해당 이메일 주소
<email_address>	별칭이 매핑될 이메일 주소. 단일 별칭이 여러 이메일 주소에 매핑될 수 있습니다.
<filename>	별칭 테이블 가져오기/내보내기에 사용할 파일 이름

archivemessage

설명

큐에서 오래된 메시지를 아카이빙합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 오래된 메시지를 아카이빙합니다.

```
mail3.example.com>
archivemessage
Enter the MID to archive.
[0]> 47
```

```
MID 47 has been saved in file oldmessage_47.mbox in the configuration
```

altsrchoost

설명

Virtual Gateway(tm) 매핑을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 altsrchoost 테이블을 인쇄하여 기존 매핑이 없음을 보여줍니다. 두 항목이 생성됩니다.

- @exchange.example.com이라는 그룹웨어 서버 호스트에서 보낸 메일이 PublicNet 인터페이스에 매핑됩니다.
- 발신자 IP 주소 192.168.35.35에서 보낸 메일은 AnotherPublicNet 인터페이스에 매핑됩니다.

마지막으로 altsrchoost 매핑을 인쇄하여 확인하고 변경 사항을 커밋합니다.

```
mail3.example.com> altsrchoost
There are currently no mappings configured.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
[ ]> new
Enter the Envelope From address or client IP address for which you want to set up a Virtual
Gateway mapping.
Partial addresses such as "@example.com" or "user@" are allowed.
[ ]> @exchange.example.com
Which interface do you want to send messages for @exchange.example.com from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 4
Mapping for @exchange.example.com on interface PublicNet created.
Choose the operation you want to perform:
```

```

- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> new
Enter the Envelope From address or client IP address for which you want to set up a Virtual
Gateway mapping.
Partial addresses such as "@example.com" or "user@" are allowed.
[]> 192.168.35.35
Which interface do you want to send messages for 192.168.35.35 from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 1
Mapping for 192.168.35.35 on interface AnotherPublicNet created.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> print
1. 192.168.35.35 -> AnotherPublicNet
2. @exchange.example.com -> PublicNet
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added 2 altsrchoost mappings
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

bounceconfig

설명

바운스의 동작을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 인라인 CLI 도움말을 참조하십시오. 이 명령의 인라인 도움말에 액세스하려면 **help** 명령을 사용합니다.

예

다음 예에서는 **bounceconfig** 명령을 사용하여 bounceprofile이라는 반송 프로파일을 생성합니다. 이 프로파일에서, 하드 반송된 모든 메시지는 대체 주소인 **bounce-mailbox@example.com**으로 전송됩니다. 지연 경고 메시지가 활성화됩니다. 경고 메시지가 수신자별로 하나씩 보내지고 경고 메시지 간격의 기본값인 4시간(14400초)이 적용됩니다.

```
mail3.example.com> bounceconfig
Current bounce profiles:
1. Default
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
[ ]> new
Please create a name for the profile:
[ ]> bounceprofile
Please enter the maximum number of retries.
[100]> 100
Please enter the maximum number of seconds a message may stay in the queue before being
hard bounced.
[259200]> 259200
Please enter the initial number of seconds to wait before retrying a message.
[60]> 60
Please enter the maximum number of seconds to wait before retrying a message.
[3600]> 3600
Do you want a message sent for each hard bounce? (Yes/No/Default) [Y]> y
Do you want bounce messages to use the DSN message format? (Yes/No/Default) [Y]> y
Enter the subject to use:
[Delivery Status Notification (Failure)]>
Select default notification template:
1. System Generated
2. bounce_english
3. bounce_russian
[1]>
Do you want to configure language specific templates? [N]>
Do you want to parse the DSN "Status" field received from bounce
responses to include in the DSN generated by the appliance?
(Yes/No/Default) [N]>
If a message is undeliverable after some interval, do you want to send a delay warning
message? (Yes/No/Default) [N]> y
Enter the subject to use:
[Delivery Status Notification (Delay)]>
Select default notification template:
1. System Generated
2. bounce_english
3. bounce_russian
[1]> 1
Do you want to configure language specific templates? [N]>
Please enter the minimum interval in seconds between delay warning messages.
[14400]> 14400
Please enter the maximum number of delay warning messages to send per
recipient.
[1]> 1
Do you want hard bounce and delay warning messages sent to an alternate address, instead
of the sender? [N]> y
Please enter the email address to send hard bounce and delay warning.
[ ]> bounce-mailbox@example.com
Do you want bounce messages to be signed (Yes/No/Default)? [N]>
Current bounce profiles:
1. Default
2. bounceprofile
```

```

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
[]>
mail3.example.com>

```

리스너에 바운스 프로필 적용

바운스 프로필을 구성한 다음 `listenerconfig` -> `bounceconfig` 명령을 사용하고 변경 사항을 커밋하는 방법으로 각 리스너에 프로필을 적용할 수 있습니다.



참고 바운스 프로필은 메시지를 수신하는 리스너에 따라 적용할 수 있습니다. 그러나 이 리스너는 메시지가 최종적으로 전달되는 방식과 무관합니다.

이 예에서는 `OutboundMail` 전용 리스너를 수정하고 `bouncepr1`이라는 바운스 프로필을 이 리스너에 적용합니다.

```

mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 2
Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> bounceconfig
Please choose a bounce profile to apply:
1. Default
2. bouncepr1
3. New Profile
[1]> 2
Name: OutboundMail

```

```

Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: bouncepr1
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Enabled the bouncepr1 profile to the Outbound mail listener
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

bouncerecipients

설명

큐의 메시지를 바운스합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

바운스할 수신자는 목적지 수신자 호스트 또는 메시지 발신자로 식별합니다. 후자의 경우 메시지 엔벨로프의 **Envelope From** 라인에 지정된 주소로 식별됩니다. 또는 전달 대기열에 있는 모든 메시지를 동시에 삭제할 수 있습니다.

수신자 호스트별 반송

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
Please enter the hostname for the messages you wish to bounce.
[]> example.com
Are you sure you want to bounce all messages being delivered to "example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

Envelope From 주소별 반송

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2
Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com
Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

모두 반송

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
Are you sure you want to bounce all messages in the queue? [N]> Y
Bouncing messages, please wait.
1000 messages bounced.
```

bvconfig

설명

바운스 확인을 위한 설정을 구성합니다. 키 및 잘못된 바운스 이메일을 구성하려면 이 명령을 사용합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 키 컨피그레이션 및 잘못된 바운스 이메일에 대해 구성된 설정을 보여줍니다.

```
mail3.example.com> bvconfig
Behavior on invalid bounces: reject
Key for tagging outgoing mail: key
Previously-used keys for verifying incoming mail:
  1. key (current outgoing key)
  2. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)
Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]> key
Enter the key to tag outgoing mail with (when tagging is enabled in the Good
Neighbor Table)
[]> basic_key
Behavior on invalid bounces: reject
Key for tagging outgoing mail: basic_key
Previously-used keys for verifying incoming mail:
  1. basic_key (current outgoing key)
  2. key (last in use Wed May 31 23:22:49 2006 GMT)
  3. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)
Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]> setup
How do you want bounce messages which are not addressed to a valid tagged
recipient to be handled?
  1. Reject.
  2. Add a custom header and deliver.
[1]> 1
Behavior on invalid bounces: reject
Key for tagging outgoing mail: basic_key
Previously-used keys for verifying incoming mail:
  1. basic_key (current outgoing key)
  2. key (last in use Wed May 31 23:22:49 2006 GMT)
  3. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)
Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Configuring a new key and setting reject for invalid email bounces
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

deleterecipients

설명

큐에서 메시지를 삭제합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

어플라이언스는 필요에 따라 수신자를 삭제할 수 있도록 다양한 옵션을 제공합니다. 다음 예에서는 수신자 호스트를 기준으로 수신자를 삭제하고 Envelope From 주소를 기준으로 삭제하고 큐의 모든 수신자를 삭제합니다.

수신자 도메인별 삭제

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
Please enter the hostname for the messages you wish to delete.
[]> example.com
Are you sure you want to delete all messages being delivered to "example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

Envelope From 주소별 삭제

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com
Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

모두 삭제

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
Are you sure you want to delete all messages in the queue? [N]> Y
Deleting messages, please wait.
1000 messages deleted.
```

deliveryconfig

설명

메일 전달을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 `deliveryconfig` 명령을 사용하여 기본 인터페이스를 "Auto"로 설정합니다. "Possible Delivery"는 활성화 상태입니다. 시스템 전체 최대 아웃바운드 메시지 전달 연결은 9,000개로 설정됩니다.

```
mail3.example.com> deliveryconfig
Choose the operation you want to perform:
- SETUP - Configure mail delivery.
[ ]> setup
Choose the default interface to deliver mail.
1. Auto
2. AnotherPublicNet (192.168.3.1/24: mail4.example.com)
3. Management (192.168.42.42/24: mail3.example.com)
4. PrivateNet (192.168.1.1/24: mail3.example.com)
5. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enable "Possible Delivery" (recommended)? [Y]> y
Please enter the default system wide maximum outbound message delivery
concurrency
[10000]> 9000
mail3.example.com>
```

delivernow

설명

즉시 전송하기 위해 메시지 일정을 조정합니다. 사용자는 단일 수신자 호스트를 선택하거나 현재 전송 예정인 모든 메시지를 선택할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> delivernow
Please choose an option for scheduling immediate delivery.
1. By recipient domain
2. All messages
[1]> 1
Please enter the recipient domain to schedule for delivery.
[]>foo.com
Scheduling all messages to foo.com for delivery.
```

destconfig

이전에는 **setgoodtable** 명령이었습니다. 이 테이블은 이제 Destination Control Table(목적지 제어 테이블)이라고 합니다. 지정된 도메인의 전달 한도를 구성할 때 이 테이블을 사용합니다.

destconfig 명령 사용

destconfig 하위 메뉴에서 다음 명령을 사용할 수 있습니다.

표 7: destconfig 하위 명령

Syntax	설명
SETUP	전역 설정을 변경합니다.
NEW	도메인에 대해 새 한도를 추가합니다.
EDIT	도메인에 대한 한도를 수정합니다.
DELETE	도메인에 대한 한도를 삭제합니다.
DEFAULT	지정되지 않은 도메인에 대한 기본 한도를 변경합니다.
LIST	도메인 및 그 한도의 목록을 표시합니다.
DETAIL	한 목적지 또는 모든 항목의 세부 사항을 표시합니다.
CLEAR	테이블에서 모든 항목을 삭제합니다.
IMPORT	.INI 컨피그레이션 파일에서 목적지 제어 항목의 테이블을 가져옵니다.
EXPORT	목적지 제어 항목의 테이블을 .INI 컨피그레이션 파일에 내보냅니다.

destconfig 명령에서는 목적지 제어 테이블의 각 행에서 다음 정보가 필요합니다.

- 도메인(수신자 호스트)
- 도메인과의 최대 동시 연결
- 연결별 메시지 한도

- 수신자 한도
- 시스템 전체 또는 Virtual Gateway 스위치
- 도메인별 제한 적용
- 수신자에 대한 기간 한도(분)
- 바운스 확인
- 도메인에 사용할 바운스 프로필

샘플 목적지 제어 테이블

다음 테이블에서는 목적지 제어 테이블의 항목을 보여줍니다.

표 8: 목적지 제어 항목의 예

도메인	연결 한도	수신자 한도	최소 기간	MX/DOM 시행
(기본)	500	없음	1	도메인
목록에 없는 도메인은 수신자/시간 제한 없이 자체적으로 500건의 연결을 갖습니다.				
(기본)	500	없음	1	MXIP
목록에 없는 도메인의 메일 게이트웨이는 수신자/시간 제한 없이 최대 500건의 연결을 갖습니다.				
partner.com	10	500	60	도메인
partner.com의 모든 도메인이 10건의 연결을 공유하며, 수신자/시간 최대값은 500입니다.				
101.202.101.2	500	없음	0	MXIP
IP 주소 지정				

배치 형식

destconfig 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 새 목적지 제어 테이블 생성

```
destconfig new <profile> [options]
```

- 기존 목적지 제어 테이블 수정

```
destconfig edit <default|profile> [options]
```

- 기존 목적지 제어 테이블 삭제

```
destconfig delete <profile>
```

- 모든 목적지 제어 항목의 요약 표시

```
destconfig list
```

- 단일 목적지 또는 모든 항목의 세부 사항 표시

```
destconfig detail <default|profile|all>
```

- 모든 기존 목적지 제어 테이블 항목 삭제

```
destconfig clear
```

- 파일에서 테이블 가져오기

```
destconfig import <filename>
```

- 파일에 테이블 내보내기

```
destconfig export <filename>
```

edit 및 **new** 배치 명령의 경우 변수 이름 및 등호 기호와 함께 값을 나타내는 방법으로 다음 옵션 중 하나 또는 모두를 제공할 수 있습니다. 지정되지 않은 옵션은 수정되지 않거나(**edit** 사용 시) 기본값으로 설정됩니다(**new** 사용 시).

`concurrency_limit=<int>` - The maximum concurrency for a specific host.

`concurrency_limit_type=<host|MXIP>` - Maximum concurrency is per host or per MX IP.

`concurrency_limit_apply=<system|VG>` - Apply maximum concurrency is system wide or by Virtual Gateway (tm).

`max_messages_per_connection=<int>` - The maximum number of messages that will be sent per connection.

`recipient_limit_minutes=<int>` - The time frame to check for recipient limits in minutes.

`recipient_limit=<int>` - The number of recipients to limit per unit of time.

`use_tls=<off|on|require|on_verify|require_verify>` - Whether TLS should be on, off, or required for a given host.

`bounce_profile=<default|profile>` - The bounce profile name to use.

```
bounce_verification=<off|on> - Bounce Verification option.
```

예: 새 **destconfig** 항목 생성

다음 예에서는 현재 **destconfig** 항목을 화면에 인쇄합니다. 그런 다음 도메인 **partner.com**의 새 항목을 생성합니다. 그 도메인에 대해 60분의 시간에 대한 동시 연결 한도 100 및 동시 수신자 한도 50이 설정됩니다. 그러면 시스템에서 지정된 1시간 동안 도메인 **partner.com**에 100건을 초과하는 연결을 열거나 50명을 초과하는 수신자에게 전달하지 않습니다. 이 도메인에는 바운스 프로파일 지정되지 않으며 특정 TLS 설정도 구성되지 않습니다. 마지막으로, 변경 사항을 인쇄하여 확인하고 커밋합니다.

```
mail3.example.com> destconfig
There are currently 2 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[ ]> list
1
Domain          Rate          Bounce          Bounce
Limiting        TLS           Verification    Profile
=====
(Default) On      Off            Off             (Default)
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[ ]> new
Enter the domain you wish to configure.
[ ]> partner.com
Do you wish to configure a concurrency limit for partner.com? [Y]> y
Enter the max concurrency limit for "partner.com".
[500]> 100
Do you wish to apply a messages-per-connection limit to this domain? [N]> n
Do you wish to apply a recipient limit to this domain? [N]> y
Enter the number of minutes used to measure the recipient limit.
[60]> 60
Enter the max number of recipients per 60 minutes for "partner.com".
[ ]> 50
Select how you want to apply the limits for partner.com:
1. One limit applies to the entire domain for partner.com
2. Separate limit for each mail exchanger IP address
[1]> 1
Select how the limits will be enforced:
1. System Wide
```

```

2. Per Virtual Gateway(tm)
[1]> 1
Do you wish to apply a specific TLS setting for this domain? [N]> n
Do you wish to apply a specific bounce verification address tagging setting for
this domain? [N]> n
Do you wish to apply a specific bounce profile to this domain? [N]> n
There are currently 3 entries configured.
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Throttled delivery to partner.com in the destconfig table
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

예: 바운스 프로파일 및 TLS 설정

이 예에서는 도메인 `newpartner.com`에 대해 새 `destconfig` 항목을 구성합니다. TLS 연결이 필요합니다. 또한 이 예에서는 `newpartner.com` 도메인에 대한 모든 이메일 전달에 사용하도록 구성된 `bouncepr1`이라는 반송 프로파일을 보여 줍니다([리스너에 바운스 프로파일 적용, 161 페이지](#) 참고).

```

mail3.example.com> destconfig
There is currently 1 entry configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new
Enter the domain you wish to configure.
[]> newpartner.com
Do you wish to configure a concurrency limit for newpartner.com? [Y]> n
Do you wish to apply a messages-per-connection limit to this domain? [N]> n
Do you wish to apply a recipient limit to this domain? [N]> n
Do you wish to apply a specific TLS setting for this domain? [N]> y
Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred(Verify)
5. Required(Verify)
[1]> 3
You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there is
a valid certificate configured.
Do you wish to apply a specific bounce verification address tagging setting for this domain?
[N]> y
Perform bounce verification address tagging? [N]> y
Do you wish to apply a specific bounce profile to this domain? [N]> y
Please choose a bounce profile to apply:
1. Default
2. New Profile
[1]> 1
There are currently 2 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.

```

예: 인바운드 “완충제”

```

- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[> detail
Domain                Rate          Bounce          Bounce
Limiting  TLS          Verification  Profile
=====  =====  =====  =====
newpartner.com  Default    Req          On          Default
(Default)      On          Off          Off         (Default)
Enter the domain name to view, or enter DEFAULT to view details for the
default, or enter ALL to view details for all:
[> all
newpartner.com
Maximum messages per connection: Default
Rate Limiting: Default
TLS: Required
Bounce Verification Tagging: On
Bounce Profile: Default
Default
Rate Limiting:
500 concurrent connections
No recipient limit
Limits applied to entire domain, across all virtual gateways
TLS: Off
Bounce Verification Tagging: Off
There are currently 2 entries configured.
[>
mail3.example.com> commit
Please enter some comments describing your changes:
[> enabled TLS for delivery to newpartner.com using demo certificate
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

예: 인바운드 “완충제”

이 예에서는 내부 그룹웨어 서버 `exchange.example.com`에 대한 메일을 제한하기 위해 또 다른 **destconfig** 항목을 생성합니다. 이 내부 서버를 위한 “shock absorber(완충제)” 항목은 특히 트래픽의 양이 많은 시기에 내부 그룹웨어 서버에 대한 인바운드 전달을 제한합니다. 이 예에서 어플라이언스는 지정된 시간(분) 동안 내부 그룹웨어 서버 `exchange.example.com`에 10건을 초과하는 연결을 열지 않고 1,000명을 초과하는 수신자에게 전달하지 않습니다. 바운스 프로필 또는 TLS 설정은 구성되지 않았습니다.

```

mail3.example.com> destconfig
There are currently 2 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[> new

```



```

Enter the domain you wish to configure.
[]> exchange.example.com
Do you wish to configure a concurrency limit for exchange.example.com? [Y]> y
Enter the max concurrency limit for "exchange.example.com".
[500]> 10
Do you wish to apply a recipient limit to this domain? [N]> y
Enter the number of minutes used to measure the recipient limit.
[60]> 1
Enter the max number of recipients per 1 minutes for "exchange.example.com".
[]> 1000
Select how you want to apply the limits for exchange.example.com:
1. One limit applies to the entire domain for exchange.example.com
2. Separate limit for each mail exchanger IP address
[1]> 1
Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1
Do you wish to apply a specific TLS setting for this domain? [N]> n
Do you wish to apply a specific bounce verification address tagging setting for this domain?
[N]> n
Do you wish to apply a specific bounce profile to this domain? [N]> n
There are currently 3 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> set up shock absorber for inbound mail
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

예: 전역 설정

이 예에서는 TLS 연결에 대한 TLS 알림 및 인증서를 구성합니다.

```

mail3.example.com> destconfig
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> setup
The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure.
1. partner.com
2. Demo

```

예: DANE 지원을 사용하여 TLS 연결 활성화

```
Please choose the certificate to apply:
[1]> 1
Do you want to send an alert when a required TLS connection fails? [N]> n
```

예: DANE 지원을 사용하여 TLS 연결 활성화

이 예에서는 newpartner.com 도메인에 대해 새 destconfig 항목을 구성합니다. 여기서, TLS 연결은 "Opportunistic" DANE 지원으로 활성화됩니다.



참고 DANE 프롬프트를 활성화하려면 TLS 지원 옵션을 선택해야 합니다.

```
mail3.example.com> destconfig
There are currently 1 entries configured. Choose the operation you want to perform:

- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

[ ]> new

Enter the domain you wish to configure.[ ]> newpartner.com
Do you want to configure a concurrency limit for newpartner.com? [Y]>
Enter the max concurrency limit for "newpartner.com".
[500]>

Do you want to apply a messages-per-connection limit to this domain? [N]>
Do you want to apply a recipient limit to this domain? [N]>
Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)

[1]>
Do you wish to apply a specific TLS setting for this domain? [N]> y
Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
6. Required - Verify Hosted Domains

[2]> 3
You have chosen to enable TLS.
Please use the 'certconfig' command to ensure that there is a valid certificate configured.
Do you want to configure DANE Support? [N]> y
Info:
If you configure DANE as 'Opportunistic' and the remote host does not support DANE,
opportunistic TLS is preferred for encrypting SMTP conversations.

If you configure DANE as 'Mandatory' and the remote host does not support DANE,
no connection is established to the destination host.
```

If you configure DANE as 'Mandatory' or 'Opportunistic' and the remote host supports DANE, it is preferred for encrypting SMTP conversations.

Please choose a DANE option:

1. No
2. Opportunistic
3. Mandatory

[2]> 2

Do you want to apply a specific bounce verification address tagging setting for this domain?
[N]>

hostrate

설명

특정 호스트의 활동을 모니터링합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> hostrate
Recipient host:
[]> aol.com
Enter the number of seconds between displays.
[10]> 1
  Time      Host  CrtCncOut  ActvRcp ActvRcp  DlvRcp  HrdBncRcp  SftBncEvt
      Status                Delta    Delta    Delta    Delta
23:38:23    up      1          0        0        4         0         0
23:38:24    up      1          0        0        4         0         0
23:38:25    up      1          0        0       12         0         0
^C
```

Ctrl-C를 누르면 hostrate 명령을 중지할 수 있습니다.

hoststatus

설명

해당 호스트 이름의 상태를 확인합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.
 배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> hoststatus

Recipient host:
[ ]> aol.com
Host mail status for: 'aol.com'
Status as of:      Fri Aug  8 11:12:00 2003
Host up/down:     up
Counters:
  Queue
    Soft Bounced Events          0
  Completion
    Completed Recipients          1
    Hard Bounced Recipients      1
      DNS Hard Bounces            0
      5XX Hard Bounces            1
    Filter Hard Bounces           0
    Expired Hard Bounces          0
    Other Hard Bounces            0
    Delivered Recipients          0
    Deleted Recipients            0
  Gauges:
    Queue
      Active Recipients           0
      Unattempted Recipients      0
      Attempted Recipients        0
    Connections
      Current Outbound Connections 0
      Pending Outbound Connections 0
  Oldest Message      No Messages
  Last Activity       Fri Aug  8 11:04:24 2003
  Ordered IP addresses: (expiring at Fri Aug  8 11:34:24 2003)
    Preference  IPs
    15          64.12.137.121    64.12.138.89    64.12.138.120
    15          64.12.137.89     64.12.138.152   152.163.224.122
    15          64.12.137.184    64.12.137.89    64.12.136.57
    15          64.12.138.57     64.12.136.153   205.188.156.122
    15          64.12.138.57     64.12.137.152   64.12.136.89
    15          64.12.138.89     205.188.156.154 64.12.138.152
    15          64.12.136.121    152.163.224.26  64.12.137.184
    15          64.12.138.120    64.12.137.152   64.12.137.121
  MX Records:
    Preference  TTL      Hostname
    15          52m24s  mailin-01.mx.aol.com
    15          52m24s  mailin-02.mx.aol.com
    15          52m24s  mailin-03.mx.aol.com
    15          52m24s  mailin-04.mx.aol.com
  Last 5XX Error:
  -----
  550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
  (at Fri Aug  8 11:04:25 2003)
  -----
  Virtual gateway information:
  =====
  example.com (PublicNet_017):
    Host up/down:  up
    Last Activity  Wed Nov 13 13:47:02 2003
```

```

Recipients 0
=====
example.com (PublicNet_023):
  Host up/down: up
  Last Activity  Wed Nov 13 13:45:01 2003
  Recipients

```

imageanalysisconfig

설명

IronPort 이미지 분석 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail.example.com>imageanalysisconfig
IronPort Image Analysis: Enabled
Image Analysis Sensitivity: 65
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
Skip small images with size less than 100 pixels (width or height)

(First time users see the license agreement displayed here.)
Choose the operation you want to perform:
- SETUP - Configure IronPort Image Analysis.
[ ]> setup
IronPort Image Analysis: Enabled
Would you like to use IronPort Image Analysis? [Y]>
Define the image analysis sensitivity. Enter a value between 0 (least sensitive) and 100
(most sensitive). As sensitivity increases, so does the false
positive rate. The default setting of 65 is recommended.
[65]>
Define the range for a CLEAN verdict. Enter the upper bound of the CLEAN range by entering
a value between 0 and 98. The default setting of 49 is
recommended.
[49]>
Define the range for a SUSPECT verdict. Enter the upper bound of the SUSPECT range by
entering a value between 50 and 99. The default setting of 74 is
recommended.
[74]>
Would you like to skip scanning of images smaller than a specific size? [Y]>
Please enter minimum image size to scan in pixels, representing either height or width of
a given image.
[100]>
IronPort Image Analysis: Enabled
Image Analysis Sensitivity: 65
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
Skip small images with size less than 100 pixels (width or height)
Choose the operation you want to perform:
- SETUP - Configure IronPort Image Analysis.
[ ]>

```

oldmessage

설명

시스템에서 가장 오래된 비-격리 메시지의 중간과 헤더를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 더 오래된 메시지가 표시됩니다.

```
mail3.example.com>
oldmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from test02.com ([172.19.0.109])
by test02.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@test02.com
To: 4031@example.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@test02.com>
```

rate

설명

메시지 처리량을 모니터링합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1
Hit Ctrl-C to return to the main prompt.
Time      Connections Recipients      Recipients      Queue
          In    Out   Received    Delta Completed    Delta    K-Used
23:37:13   10    2   41708833     0   40842686     0      64
23:37:14    8    2   41708841     8   40842692     6     105
```

```

23:37:15      9      2      41708848      7      40842700      8      76
23:37:16      7      3      41708852      4      40842705      5      64
23:37:17      5      3      41708858      6      40842711      6      64
23:37:18      9      3      41708871      13     40842722      11     67
23:37:19      7      3      41708881      10     40842734      12     64
23:37:21     11      3      41708893      12     40842744      10     79
^C

```

redirectrecipients

설명

다른 릴레이 호스트에 모든 메시지를 리디렉션합니다.



위험 목적지가 /dev/null인 수신 도메인에 메시지를 리디렉션하면 메시지를 잃게 됩니다. 그런 도메인으로 메일을 리디렉션하면 CLI에서 경고를 표시하지 않습니다. 메시지를 리디렉션하기 전에 수신 도메인에 대한 SMTP 경로를 확인합니다.



위험 이 호스트에서 보내는 대량의 SMTP 메일을 수락할 준비가 되지 않은 호스트 또는 IP 주소에 수신자를 리디렉션하면 메시지가 바운스되며 메일을 잃게 될 수도 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

redirectrecipients 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 다른 호스트 이름 또는 IP 주소에 모든 메일 리디렉션

```
redirectrecipients host <hostname>
```

예

다음 예는 모든 메일을 example2.com 호스트로 리디렉션합니다.

```

mail3.example.com> redirectrecipients
Please enter the hostname or IP address of the machine you want to send all mail to.
[ ]> example2.com
WARNING: redirecting recipients to a host or IP address that is not prepared to accept large
volumes of SMTP mail from this host

```

```
will cause messages to bounce and possibly result in the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
Redirecting messages, please wait.
246 recipients redirected.
```

resetcounters

설명

시스템의 모든 카운터를 재설정합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

removemessage

설명

지정된 메시지 ID의 메시지를 안전하게 삭제하려고 시도합니다.

removemessage 명령은 작업 대기열, 재시도 대기열 또는 대상 대기열에 있는 메시지만 제거할 수 있습니다. 시스템의 상태에 따라 유효하고 활성 상태인 메시지가 이 큐 중 어디에도 있지 않을 가능성이 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
example.com>
removemessage
Enter the MID to remove.
[]> 1
MID 1: 19 secs old
Received: from example2.com ([172.16.0.102])
  by test02.com with SMTP; 01 Mar 2007 19:50:41 -0800
```



```

From: user123@test02.com
To: 9526@example.com
Subject: Testing
Message-Id: <20070302035041.67424.53212@test02.com>
Remove this message? [N]> y

```

showmessage

설명

지정된 메시지 ID의 메시지 및 메시지 본문을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

example.com> showmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from example2.com([172.19.0.109])
  by test02.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@test02.com
To: 4031@example.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@test02.com>
This is the message body.

```

showrecipients

설명

큐의 메시지를 수신자 호스트 기준으로 또는 Envelope From 주소 기준으로 표시하거나 모두 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

showrecipients 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 수신자 호스트 이름을 기준으로 메시지를 찾습니다.

```
showrecipients host <hostname>
```

- Envelope From 주소를 기준으로 메시지 찾기

```
showrecipients [sender_options] <sender_email>
```

다음 sender_option을 사용할 수 있습니다.

--match-case 주소의 사용자 이름 부분에 대한 대/소문자 구분 매치

- 모든 메시지 찾기

```
showrecipients all
```

예

다음 예는 모든 수신자 호스트에 대한 대기열의 메시지를 표시합니다.

```
mail3.example.com> showrecipients
Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
Showing messages, please wait.
MID/      Bytes/      Sender/      Subject
[RID]     [Atmps]    Recipient
1527      1230       user123456@ironport.com Testing
[0]       [0]        9554@example.com
1522      1230       user123456@ironport.com Testing
[0]       [0]        3059@example.com
1529      1230       user123456@ironport.com Testing
[0]       [0]        7284@example.com
1530      1230       user123456@ironport.com Testing
[0]       [0]        8243@example.com
1532      1230       user123456@ironport.com Testing
[0]       [0]        1820@example.com
1531      1230       user123456@ironport.com Testing
[0]       [0]        9595@example.com
1518      1230       user123456@ironport.com Testing
[0]       [0]        8778@example.com
1535      1230       user123456@ironport.com Testing
[0]       [0]        1703@example.com
1533      1230       user123456@ironport.com Testing
[0]       [0]        3052@example.com
1536      1230       user123456@ironport.com Testing
[0]       [0]        511@example.com
```

status

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> status detail
```

```
Status as of:                Mon Sep 08 00:01:44 2014 GMT
Up since:                   Tue Aug 26 17:24:16 2014 GMT
(12d 6h 37m 28s)
Last counter reset:        Never
System status:             Online
Oldest Message:           No Messages
Feature - IronPort Anti-Spam: 1459 days
Feature - Incoming Mail Handling: Perpetual
Feature - Outbreak Filters: 1459 days

Counters:
      Reset                Uptime                Lifetime
Receiving
  Messages Received                2                2                2
  Recipients Received              2                2                2
Rejection
  Rejected Recipients              0                0                0
  Dropped Messages                 0                0                0
Queue
  Soft Bounced Events             0                0                0
Completion
  Completed Recipients             0                0                0
Current IDs
  Message ID (MID)                                2
  Injection Conn. ID (ICID)                      0
  Delivery Conn. ID (DCID)                        13

Gauges:
      Current
Connections
  Current Inbound Conn.                0
  Current Outbound Conn.               0
Queue
  Active Recipients                    2
  Messages In Work Queue               0
  Kilobytes Used                       184
  Kilobytes Free                       8,388,424
Quarantine
  Messages In Quarantine
    Policy, Virus and Outbreak        0
  Kilobytes In Quarantine
    Policy, Virus and Outbreak        0
```

tophosts

설명

이메일 대기열에 대한 즉각적인 정보를 얻고 특정 수신자 호스트에 전달 문제(예: 대기열 빌드업)가 있는지를 확인하려면 **tophosts** 명령을 사용합니다. **tophosts** 명령은 대기열에 있는 상위 20 수신자 호스트 목록을 반환합니다. 활성 수신자, 연결 발신, 전달된 수신자, 소프트 반송된 이벤트, 하드 반송된 수신자 등 여러 통계를 기준으로 목록을 정렬할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> tophosts
Sort results by:
1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]> 1
Status as of: Fri Mar 13 06:09:18 2015 GMT
Hosts marked with '*' were down as of the last delivery attempt.
```

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard Bounced
1*	example.com	2	0	0	0	0
2	the.encryption.queue	0	0	0	0	0
3	the.euq.queue	0	0	0	0	0
4	the.euq.release.queue	0	0	0	0	0

topin

설명

수신 연결 수를 기준으로 최상위 호스트를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> topin
```

```
Status as of:                Sat Aug 23 21:50:54 2003
# Remote hostname           Remote IP addr.  listener        Conn. In
1mail.remotedomain01.com    172.16.0.2      Incoming01      10
2 mail.remotedomain01.com    172.16.0.2      Incoming02      10
3 mail.remotedomain03.com    172.16.0.4      Incoming01      5
4 mail.remotedomain04.com    172.16.0.5      Incoming02      4
5 mail.remotedomain05.com    172.16.0.6      Incoming01      3
6 mail.remotedomain06.com    172.16.0.7      Incoming02      3
7 mail.remotedomain07.com    172.16.0.8      Incoming01      3
8 mail.remotedomain08.com    172.16.0.9      Incoming01      3
9 mail.remotedomain09.com    172.16.0.10     Incoming01      3
10 mail.remotedomain10.com   172.16.0.11     Incoming01      2
11 mail.remotedomain11.com   172.16.0.12     Incoming01      2
12 mail.remotedomain12.com   172.16.0.13     Incoming02      2
13 mail.remotedomain13.com   172.16.0.14     Incoming01      2
14 mail.remotedomain14.com   172.16.0.15     Incoming01      2
15 mail.remotedomain15.com   172.16.0.16     Incoming01      2
16 mail.remotedomain16.com   172.16.0.17     Incoming01      2
17 mail.remotedomain17.com   172.16.0.18     Incoming01      1
18 mail.remotedomain18.com   172.16.0.19     Incoming02      1
19 mail.remotedomain19.com   172.16.0.20     Incoming01      1
20 mail.remotedomain20.com   172.16.0.21     Incoming01      1
```

unsubscribe

설명

전역 수신 거부 목록을 업데이트합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 주소 `user@example.net`이 전역 수신 거부 목록에 추가되고, 메시지를 하드 반송하도록 기능이 구성됩니다. 이 주소로 전송된 메시지는 반송됩니다. 어플라이언스는 전달 직전에 메시지를 반송합니다.

```
mail3.example.com> unsubscribe
Global Unsubscribe is enabled. Action: drop.
Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import entries from a file.
- SETUP - Configure general settings.
[]> new
Enter the unsubscribe key to add. Partial addresses such as "@example.com"
or "user@" are allowed, as are IP addresses. Partial hostnames such as "@.example.com" are
```

```

    allowed.
[ ]> user@example.net
Email Address 'user@example.net' added.
Global Unsubscribe is enabled. Action: drop.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[ ]> setup
Do you want to enable the Global Unsubscribe feature? [Y]> y
Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2
Global Unsubscribe is enabled. Action: bounce.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[ ]>
mail3.example.com> commit
Please enter some comments describing your changes:
[ ]> Added username "user@example.net" to global unsubscribe
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

workqueue

설명

작업 큐 일시 중지 상태를 표시하거나 변경합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> workqueue
Status: Operational
Messages: 1243
Manually pause work queue? This will only affect unprocessed messages. [N]> y
Reason for pausing work queue:
[ ]> checking LDAP server
Status: Paused by admin: checking LDAP server
Messages: 1243

```



참고 이유를 입력하는 것은 선택 사항입니다. 이유를 입력하지 않으면 시스템에서는 "operator paused(운영자가 일시 중지)"라고 기록합니다.

이 예에서는 작업 대기열이 다시 시작됩니다.

```
mail3.example.com> workqueue
Status:   Paused by admin: checking LDAP server
Messages: 1243
Resume the work queue?  [Y]> y
Status:   Operational
Messages: 1243
```

네트워크 컨피그레이션/네트워크 툴

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [etherconfig](#), 187 페이지
- [interfaceconfig](#), 189 페이지
- [nslookup](#), 191 페이지
- [netstat](#), 192 페이지
- [packetcapture](#), 193 페이지
- [ping](#), 194 페이지
- [ping6](#), 195 페이지
- [routeconfig](#), 196 페이지
- [setgateway](#), 198 페이지
- [sethostname](#), 199 페이지
- [smtproutes](#), 200 페이지
- [sslconfig](#), 201 페이지
- [ssl3config](#), 204 페이지
- [telnet](#), 204 페이지
- [traceroute](#), 205 페이지
- [traceroute6](#), 206 페이지

etherconfig

설명

미디어 설정, NIC 페어링, VLAN 컨피그레이션, DSR 컨피그레이션을 포함하여 이더넷 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN tag ID for the interface (Ex: "34"):
[]> 12
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
2. Data 2
3. Management
[1]> 1
VLAN interfaces:
1. VLAN 12 (Data 1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> loopback
Currently configured loopback interface:
Choose the operation you want to perform:
- ENABLE - Enable Loopback Interface.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> mtu
Ethernet interfaces:
1. Data 1 default mtu 1500
2. Data 2 default mtu 1500
3. Management default mtu 1500
4. VLAN 12 default mtu 1500
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
```



```
[ ]> edit
Enter the name or number of the ethernet interface you wish to edit.
[ ]> pair1
That value is not valid.
Enter the name or number of the ethernet interface you wish to edit.
[ ]> 12
That value is not valid.
Enter the name or number of the ethernet interface you wish to edit.
[ ]> 2
Please enter a non-default (1500) MTU value for the Data 2 interface.
[ ]> 1200
Ethernet interfaces:
1. Data 1 default mtu 1500
2. Data 2 mtu 1200
3. Management default mtu 1500
4. VLAN 12 default mtu 1500
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[ ]>
```

interfaceconfig

설명

인터페이스를 구성합니다. 인터페이스를 생성, 수정하거나 삭제할 수 있습니다. FTP를 활성화하고 IP 주소를 변경하고 이더넷 IP 주소를 구성할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

interfaceconfig 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 새 인터페이스 생성

interfaceconfig new <name>
<ethernet interface>
<hostname>
--ip=IPv4 Address/Netmask
--ip6=IPv6 Address/Prefix Length
[--ftp[=<port>]]

<code>[--telnet[=<port>]]</code>
<code>[--ssh[=<port>]]</code>
<code>[--http][=<port>]</code>
<code>[--https[=<port>]]</code>
<code>[--euq_http[=<port>]]</code>
<code>[--euq_https][=<port>]</code>
<code>[--ccs[=<port>]].</code>
FTP is available only on IPv4.

- 인터페이스 삭제

```
interfaceconfig delete <name>
```

예: 인터페이스 구성

```
mail.example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.76.69.149/24 on Management: mail.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[ ]> edit
Enter the number of the interface you wish to edit.
[ ]> 1
IP interface name (Ex: "InternalNet"):
[Management]>
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[1.1.1.1]>
Netmask (Ex: "24", "255.255.255.0" or "0xffffffff"):
[0xffffffff]>
Would you like to configure an IPv6 address for this interface (y/n)? [N]> n
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[3]>
Hostname:
[mail.example.com]>
Do you want to enable SSH on this interface? [Y]>
Which port do you want to use for SSH?
[22]>
```

```

Do you want to enable FTP on this interface? [N]>
Do you want to enable Cluster Communication Service on this interface? [N]>
Do you want to enable HTTP on this interface? [Y]>
Which port do you want to use for HTTP?
[80]>
Do you want to enable HTTPS on this interface? [Y]>
Which port do you want to use for HTTPS?
[443]>
Do you want to enable Spam Quarantine HTTP on this interface? [N]>
Do you want to enable Spam Quarantine HTTPS on this interface? [N]>
Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [N]> y
Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6080]>
Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [N]> y
Which port do you want to use for AsyncOS API (Monitoring) HTTPS?
[6443]>
The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure. To assure privacy, run "certconfig" first.
Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the
secure service? [Y]>
You have edited the interface you are currently logged into. Are you sure you want to
change it? [Y]>
Currently configured interfaces:
1. Management (10.76.69.149/24 on Management: mail.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>

```

nslookup

설명

DNS 기능을 확인하려면 **nslookup** 명령을 사용합니다.

nslookup 명령은 어플라이언스에서 작동 중인 DNS(Domain Name Service) 서버에 연결하여 호스트 이름 및 IP 주소를 확인하는 것이 가능한지 확인할 수 있습니다.

표 9: **nslookup** 명령 쿼리 유형

쿼리 유형	설명
	호스트의 인터넷 주소
CNAME	별칭(alias)에 대한 정규 이름(canonical name)
MX	메일 교환기
NS	이름이 지정된 영역의 이름 서버
PTR	쿼리가 인터넷 주소인 경우 호스트 이름, 그렇지 않은 경우 다른 정보에 대한 포인터
SOA	도메인의 "인증 기관 시작" 정보

쿼리 유형	설명
TXT	텍스트 정보

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> nslookup
Please enter the host or IP address to resolve.
[]> vm30esa0086.ibqa
Choose the query type:
1. A          the host's IP address
2. AAAA       the host's IPv6 address
3. CNAME      the canonical name for an alias
4. MX         the mail exchanger
5. NS         the name server for the named zone
6. PTR        the hostname if the query is an Internet address,
otherwise the pointer to other information
7. SOA        the domain's "start-of-authority" information
8. TXT        the text information
[1]> 2
AAAA=2001:420:54ff:ff06::95 TTL=30m
```

netstat

설명

네트워크 연결(수신 및 발신 모두), 라우팅 테이블, 네트워크 인터페이스 통계 수치를 표시하려면 **netstat** 명령을 사용합니다. 이 버전에서 모든 인수를 지원하지는 않습니다. 특히 **-a**, **-A**, **-g**, **-m**, **-M**, **-N**, **-s**를 사용할 수 없습니다. 이 명령은 대화형 모드에서 실행해야 하므로 **netstat**를 입력한 다음 5가지 보고 옵션 중에서 선택할 수 있습니다. 또한 수신할 인터페이스 및 표시 간격을 지정할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
example.com> netstat
Choose the information you want to display:
1. List of active sockets.
```

```

2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
[1]> 2
Select the ethernet interface whose state you wish to display:
1. Data 1
2. Data 2
3. Management
4. ALL
[]> 1
Show the number of bytes in and out? [N]>
Show the number of dropped packets? [N]> y
Name      Mtu Network          Address          Ipkts Ierrs   Opkts
Oerrs  Coll Drop
Data 1 1500 197.19.1/24   example.com      30536    -     5    -
-      -
example.com>

```

packetcapture

설명

네트워크 연결(수신 및 발신 모두), 라우팅 테이블, 네트워크 인터페이스 통계 수치를 표시하려면 **netstat** 명령을 사용합니다. 이 버전에서 모든 인수를 지원하지는 않습니다. 특히 **-a**, **-A**, **-g**, **-m**, **-M**, **-N**, **-s**를 사용할 수 없습니다. 이 명령은 대화형 모드에서 실행해야 하므로 **netstat**를 입력한 다음 5가지 보고 옵션 중에서 선택할 수 있습니다. 또한 수신할 인터페이스 및 표시 간격을 지정할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail.example.com> packetcapture
Capture Information:
  Status:          No capture running
Current Settings:
  Maximum File Size: 200 MB
  Limit:           None (Run Indefinitely)
  Interface(s):    ALL
  Filter:          (tcp port 25)
Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> start
Success - Packet Capture has started
Capture Information:
  File Name:       C100V-421C73B18CFB05784A83-B03A99E71ED8-20150312-105256.cap
  File Size:       0 of 200M
  Duration:       0s

```

```

Limit:          None (Run Indefinitely)
Interface(s):   ALL
Filter:         (tcp port 25)
Choose the operation you want to perform:
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[ ]> stop
Success - Packet Capture has stopped
Capture Information:
File Name:      C100V-421C73B18CFB05784A83-B03A99E71ED8-20150312-105256.cap
File Size:      24 of 200M
Duration:       10s
Limit:          None (Run Indefinitely)
Interface(s):   ALL
Filter:         (tcp port 25)
Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[ ]> setup
Enter maximum allowable size for the capture file (in MB)
[200]>
Do you want to stop the capture when the file size is reached? (If not, a new file will be
started and the older capture data will be discarded.)
[N]>
The following interfaces are configured:
1. Management
2. ALL
Enter the name or number of one or more interfaces to capture packets from, separated by
commas (enter ALL to use all interfaces):
[2]>
Select an operation. Press enter to continue with the existing filter.
- PREDEFINED - PREDEFINED filter.
- CUSTOM - CUSTOM filter.
- CLEAR - CLEAR filter.
[ ]>
Capture settings successfully saved.
Current Settings:
Maximum File Size: 200 MB
Limit:            None (Run Indefinitely)
Interface(s):     ALL
Filter:           (tcp port 25)
Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[ ]>

```

ping

설명

ping 명령을 사용하면 어플라이언스에서 네트워크 호스트와의 연결을 테스트할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> ping
Which interface do you want to send the pings from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Please enter the host you wish to ping.
[]> anotherhost.example.com
Press Ctrl-C to stop.
PING anotherhost.example.com (
x.x.x.x
): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=0 ttl=64 time=1.421 ms
64 bytes from 10.19.0.31: icmp_seq=1 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=2 ttl=64 time=0.118 ms
64 bytes from 10.19.0.31: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 10.19.0.31: icmp_seq=4 ttl=64 time=0.139 ms
64 bytes from 10.19.0.31: icmp_seq=5 ttl=64 time=0.125 ms
64 bytes from 10.19.0.31: icmp_seq=6 ttl=64 time=0.124 ms
64 bytes from 10.19.0.31: icmp_seq=7 ttl=64 time=0.122 ms
64 bytes from 10.19.0.31: icmp_seq=8 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
^C
```



참고 ping 명령을 끝내려면 Ctrl-C를 사용해야 합니다.

ping6

설명

IPv6를 사용하는 네트워크 호스트를 ping합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> ping6
Which interface do you want to send the pings from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
[1]> 1
Please enter the host you wish to ping.
[]> anotherhost.example.com
Press Ctrl-C to stop.
```



참고 ping6 명령을 끝내려면 Control-C를 사용해야 합니다.

routeconfig

설명

routeconfig 명령을 사용하면 TCP/IP 트래픽을 위한 고정 경로를 생성, 수정, 삭제할 수 있습니다. 기본적으로 트래픽은 setgateway 명령으로 설정된 기본 게이트웨이를 통해 라우팅됩니다. 그러나 AsyncOS에서는 목적지에 따라 특정 경로를 지정할 수 있습니다.

경로는 별칭(향후 참조용), 목적지, 게이트웨이로 구성됩니다. 게이트웨이(다음 홉)는 10.1.1.2와 같은 IP 주소입니다. 목적지는

- 192.168.14.32와 같은 IP 주소 또는
- CIDR 표기의 서브넷 중 하나일 수 있습니다. 예를 들어 192.168.5.0/24는 192.168.5.0부터 192.168.5.255까지의 전체 클래스 C 네트워크를 의미합니다.

IPv6 주소는 다음 형식을 사용할 수 있습니다.

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

이 명령은 현재 구성된 모든 TCP/IP 경로의 목록을 제공합니다. 그 목록에서 edit 및 delete 하위 명령을 사용하여 선택할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

smtproutes 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다. 경로에 대해 IPv4 주소 또는 IPv6 주소를 사용하도록 선택할 수 있습니다.

- 고정 경로 생성:

```
routeconfig new 4|6 <name> <destination_address> <gateway_ip>
```

표 10: routeconfig 인수

Argument	설명
4 6	이 명령을 적용할 IP 버전(IPv4 또는 IPv6). clear 및 print에서는 이 옵션을 생략할 수 있으며, 그러면 두 버전 모두에 적용됩니다.
name	경로의 이름
destination_address	발신 IP 트래픽에 대해 매치할 IP 또는 CIDR 주소
gateway_ip	이 트래픽을 보낼 IP 주소

- 고정 경로 수정:

```
routeconfig edit 4|6 <name> <new_name> <destination_address> <gateway_ip>
```

- 고정 경로 삭제:

```
routeconfig delete 4|6 <name>
```

- 모든 고정 경로 삭제:

```
routeconfig clear [4|6]
```

- 고정 경로의 목록 인쇄:

```
routeconfig print [4|6]
```

예

```
mail3.example.com> routeconfig
Configure routes for:
1. IPv4
2. IPv6
[1]>
Currently configured routes:
Choose the operation you want to perform:
- NEW - Create a new route.
```

```

[ ]> new
Please create a name for the route:
[ ]> EuropeNet
Please enter the destination IPv4 address to match on.
CIDR addresses such as 192.168.42.0/24 are also allowed.
[ ]> 192.168.12.0/24
Please enter the gateway IP address for traffic to 192.168.12.0/24:
[ ]> 192.168.14.4
Currently configured routes:
1. EuropeNet Destination: 192.168.12.0/24 Gateway: 192.168.14.4
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[ ]>
mail3.example.com> routeconfig
Configure routes for:
1. IPv4
2. IPv6
[1]> 2
Currently configured routes:
Choose the operation you want to perform:
- NEW - Create a new route.
[ ]> new
Please create a name for the route:
[ ]> EuropeIPv6Net
Please enter the destination IPv6 address to match on.
CIDR addresses such as 2001:db8::/32 are also allowed.
[ ]> 2620:101:2004:4202::/6
Please enter the gateway IP address for traffic to 2620:101:2004:4202::/6:
[ ]> 2620:101:2004:4202::23
Currently configured routes:
1. EuropeIPv6Net Destination: 2620:101:2004:4202::/6 Gateway:
2620:101:2004:4202::23
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[ ]>

```

setgateway

설명

setgateway 명령은 패킷 라우팅에서 거쳐야 할 기본 다음 홉 중간 지점을 구성합니다. (기본이 아닌) 대체 게이트웨이는 routeconfig 명령으로 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> setgateway
Warning: setting an incorrect default gateway may cause the current connection to be
interrupted when the changes are committed.
Enter new default gateway:
[10.1.1.1]> 192.168.20.1
mail3.example.com> commit
Please enter some comments describing your changes:
[]> changed default gateway to 192.168.20.1
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

sethostname

설명

호스트 이름은 CLI 프롬프트에서 시스템을 식별하는 데 사용됩니다. 인증된 호스트 이름을 입력해야 합니다. sethostname 명령은 Email Security Appliance의 이름을 설정합니다. 새 호스트 이름은 commit 명령을 실행할 때까지 적용되지 않습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

호스트 이름 변경을 적용하려면 commit 명령을 입력해야 합니다. 호스트 이름 변경을 성공적으로 커밋하면 새 이름이 CLI 프롬프트에 나타납니다.

```
oldname.example.com> commit
Please enter some comments describing your changes:
[]> Changed System Hostname
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

다음과 같이 새 호스트 이름이 프롬프트에 나타납니다.

```
mail3.example.com>
```

smtproutes

설명

영구 도메인 리디렉션을 설정합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

smtproutes 명령의 배치 형식은 기존 CLI 명령의 모든 기능을 수행하는 데 사용할 수 있습니다.

- 새 SMTP 경로 만들기

```
smtproutes new <source> <destination> [destination] [destination] [...]
```

- 기존 SMTP 경로 삭제

```
smtproutes delete <source>
```

- SMTP 경로 목록 지우기

```
smtproutes clear
```

- SMTP 경로 목록 인쇄

```
smtproutes print
```

- SMTP 경로 목록 가져오기

```
smtproutes import <filenames>
```

- SMTP 경로 목록 내보내기

```
smtproutes export <filenames>
```

예

다음 예에서는 smtproutes 명령을 사용하여 도메인 example.com에 대한 경로(매핑)를 relay1.example.com, relay2.example.com, backup-relay.example.com으로 구성합니다. 목적지 우선 순위를 지정하려면 /pri=#을

사용합니다.#의 범위는 0-65535이며, 숫자가 클수록 우선 순위가 낮아집니다. 지정하지 않을 경우 기본 우선 순위는 0입니다.

InboundMail 공용 리스너를 구성할 때 `systemsetup` 명령에서 동일한 매핑을 생성했을 수도 있습니다.

```
mail3.example.com> smtproutes
There are no routes configured.
Choose the operation you want to perform:
- NEW - Create a new route.
- IMPORT - Import new routes from a file.
[]> new
Enter the domain for which you want to set up a permanent route.
Partial hostnames such as ".example.com" are allowed.
Use "ALL" for the default route.
[]> example.com
Enter the destination hosts, separated by commas, which you want mail
for example.com to be delivered.
Enter USEDNS by itself to use normal DNS resolution for this route.
Enter /dev/null by itself if you wish to discard the mail.
Enclose in square brackets to force resolution via address (A)
records, ignoring any MX records.
[]> relay1.example.com/pri=10, relay2.example.com, backup-relay.example.com
Mapping for example.com to relay1.example.com, relay2.example.com,
backup-relay.example.com/pri=10 created.
There are currently 1 routes configured.
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.
[]>
```

sslconfig

설명

어플라이언스를 위한 SSL 설정을 구성합니다.



참고 FIPS 140-2 규정 준수 모드에서 서버 및 클라이언트 방식을 변경할 수 없습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail.example.com> sslconfig

sslconfig settings:
  GUI HTTPS method:  tlsv1_1tlsv1_2
  GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL

  Inbound SMTP method:  tlsv1_1tlsv1_2
  Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL

  Outbound SMTP method:  tlsv1_1tlsv1_2
  Outbound SMTP ciphers:
    ECDH+aRSA
    ECDH+ECDSA
    DHE+DSS+AES
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !eNULL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[ ]> gui
Enter the GUI HTTPS ssl method you want to use.
1. TLS v1.0
2. TLS v1.1
3. TLS v1.2
4. SSL v3
[2, 3]> 1
Enter the GUI HTTPS ssl cipher you want to use.
[AES128: AES256: !SRP: !AESGCM+DH+aRSA: !AESGCM+RSA: !aNULL]>
sslconfig settings:
  GUI HTTPS method:  tlsv1_0
  GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL

  Inbound SMTP method:  tlsv1_1tlsv1_2
  Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA

```

```

!AESGCM+RSA
!aNULL
Outbound SMTP method:  tlsv1_1tlsv1_2
Outbound SMTP ciphers:
  ECDH+aRSA
  ECDH+ECDSA
  DHE+DSS+AES
  AES128
  AES256
  !SRP
  !AESGCM+DH+aRSA
  !AESGCM+RSA
  !aNULL
  !eNULL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[ ]> inbound
Enter the inbound SMTP ssl method you want to use.
1. TLS v1.0
2. TLS v1.1
3. TLS v1.2
4. SSL v3
[2, 3]> 2
Enter the inbound SMTP ssl cipher you want to use.
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL]>
  sslconfig settings:
  GUI HTTPS method:  tlsv1_0
  GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
  Inbound SMTP method:  tlsv1_1
  Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
  Outbound SMTP method:  tlsv1_1tlsv1_2
  Outbound SMTP ciphers:
    ECDH+aRSA
    ECDH+ECDSA
    DHE+DSS+AES
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !eNULL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.

```

```
- VERIFY - Verify and show ssl cipher list.
[]>
[]>
```

sslv3config

설명

어플라이언스를 위한 SSLv3 설정을 활성화하거나 비활성화합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 엔드 유저 격리를 위한 SSLv3를 비활성화하는 방법을 보여줍니다.

```
mail.example.com> sslv3config
Current SSLv3 Settings:
-----
          UPDATER      :      Enabled
    WEBSECURITY      :      Enabled
           EUQ        :      Enabled
           LDAP       :      Enabled
-----

Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]> setup
Choose the service to toggle SSLv3 settings:
1. EUQ Service
2. LDAP Service
3. Updater Service
4. Web Security Service
[1]>
Do you want to enable SSLv3 for EUQ Service ? [Y]>n
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]>
```

telnet

설명

원격 호스트에 연결합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> telnet
Please select which interface you want to telnet from.
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 3
Enter the remote hostname or IP.
[]> 193.168.1.1
Enter the remote port.
[25]> 25
Trying 193.168.1.1...
Connected to 193.168.1.1.
Escape character is '^'.
```

traceroute

설명

어플라이언스에서 IPv4를 사용하는 네트워크 호스트와의 연결을 테스트하고 네트워크 홉의 라우팅 문제를 디버깅하려면 `traceroute` 명령을 사용합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> traceroute
Which interface do you want to trace from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Please enter the host to which you want to trace the route.
[]> 10.1.1.1
Press Ctrl-C to stop.
traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets
 1 gateway
  (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms
 2 hostname
```

```
(10.1.1.1) 0.298 ms 0.302 ms 0.291 ms
mail3.example.com>
```

tracert6

설명

어플라이언스에서 IPv6를 사용하는 네트워크 호스트와의 연결을 테스트하고 네트워크 홉의 라우팅 문제를 디버깅하려면 **tracert6** 명령을 사용합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> tracert6
Which interface do you want to trace from?
1. Auto
2. D1 (2001:db8::/32: example.com)
[1]> 1
Please enter the host to which you want to trace the route.
[]> example.com
Press Ctrl-C to stop.
connect: No route to host
vm10esa0031.qa> tracert6
Which interface do you want to trace from?
1. Auto
2. D1 (2001:db8::/32: example.com)
[1]> 2
Please enter the host to which you want to trace the route.
[]> example.com
Press Ctrl-C to stop.
tracert6 to example.com (2606:2800:220:1:248:1893:25c8:1946) from 2001:db8::, 64 hops
max, 12 byte packets
sendto: No route to host
 1 tracert6: wrote example.com 12 chars, ret=-1
 *sendto: No route to host
tracert6: wrote example.com 12 chars, ret=-1
 *sendto: No route to host
tracert6: wrote example.com 12 chars, ret=-1
```

신종 바이러스 필터(Outbreak Filter)

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [outbreakconfig, 207 페이지](#)
- [outbreakflush, 208 페이지](#)

- [outbreakstatus](#), 208 페이지
- [outbreakupdate](#), 209 페이지

outbreakconfig

설명

보안 침해 필터 기능을 구성하려면 **outbreakconfig** 명령을 사용합니다. 이 명령을 사용하여 다음 작업을 수행할 수 있습니다.

- Outbreak Filter를 전역적으로 활성화
- 적용 규칙 검사 활성화
- 검사할 파일의 최대 크기 설정(크기는 바이트 단위로 입력)
- Outbreak Filter에 대한 알림 활성화
- URL 로깅 활성화

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> outbreakconfig
Outbreak Filters: Enabled
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]> setup
Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>
Outbreak Filters enabled.
Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below), meaning that new messages of
certain types could be quarantined or will no longer be quarantined, respectively.
Would you like to receive Outbreak Filter alerts? [N]>
What is the largest size message Outbreak Filters should scan?
[524288]>
Do you want to use adaptive rules to compute the threat level of messages? [Y]>
Logging of URLs is currently disabled.
Do you wish to enable logging of URL's? [N]> Y
Logging of URLs has been enabled.
The Outbreak Filters feature is now globally enabled on the system. You must use the
'policyconfig' command in the CLI or the Email
Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing
Mail Policies.
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]>
```

outbreakflush

설명

캐싱된 보안 침해 규칙을 지웁니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> outbreakflush
Warning - This command removes the current set of Outbreak Filter Rules, leaving your network
exposed until the next rule download.
Run "outbreakupdate force" command to immediately download Outbreak Filter Rules.
Are you sure that you want to clear the current rules? [N]> y
Cleared the current rules.
mail3.example.com>
```

outbreakstatus

설명

outbreakstatus 명령은 보안 침해 필터 기능의 활성화 여부, 모든 보안 침해 규칙, 현재 임계값을 포함하여 현재의 보안 침해 필터 기능 설정을 보여줍니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> outbreakstatus
Outbreak Filters: Enabled

Component                Last Update                Version
CASE Core Files           26 Jan 2014 06:45 (GMT +00:00)  3.3.1-005
CASE Utilities            26 Jan 2014 06:45 (GMT +00:00)  3.3.1-005
Outbreak Rules            26 Jan 2014 07:00 (GMT +00:00)  20140126_063240

Threat Outbreak          Outbreak
Level  Rule Name           Rule Description
-----
```

```

5  OUTBREAK_0002187_03  A reported a MyDoom.BB outbreak.
5  OUTBREAK_0005678_00  This configuration file was generated by...
3  OUTBREAK_0000578_00  This virus is distributed in pictures of...

```

Outbreak Filter Rules with higher threat levels pose greater risks.
(5 = highest threat, 1 = lowest threat)

Last update: Mon Jan 27 04:36:27 2014

mail3.example.com>

outbreakupdate

설명

CASE 규칙 및 엔진 코어에 대한 즉각적인 업데이트를 요청합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

예

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

```

elroy.run> outbreakupdate
Requesting updates for Outbreak Filter Rules.

```

정책 시행

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [dictionaryconfig, 210 페이지](#)
- [exceptionconfig, 213 페이지](#)
- [filters, 214 페이지](#)
- [policyconfig, 216 페이지](#)
- [quarantineconfig, 238 페이지](#)
- [scanconfig, 239 페이지](#)
- [stripheaders, 242 페이지](#)
- [textconfig, 243 페이지](#)

dictionaryconfig

설명

콘텐츠 사전을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

사전을 생성하려면 **dictionaryconfig -> new**를, 사전을 삭제하려면 **dictionaryconfig -> delete**를 사용합니다.

사전 생성

```
example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new
Enter a name for this content dictionary.
[]> HRWords
Do you wish to specify a file for import? [N]>
Enter new words or regular expressions, enter a blank line to finish.
<list of words typed here>
Currently configured content dictionaries:
1. HRWords
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> delete
Enter the number of the dictionary you want to delete:
1. HRWords
[]> 1
Content dictionary "HRWords" deleted.
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]>
```

사전 생성 2

이 예에서는 “codename”이라는 용어를 포함하기 위해 “secret_words”라는 새 사전을 만듭니다. 사전을 입력한 다음 **edit -> settings** 하위 명령을 사용하여 사전에 포함되는 단어에 대한 대/소문자 구분 및 단어 경계 탐지를 정의합니다.

```
mail3.example.com> dictionaryconfig
```

```

No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new
Enter a name for this content dictionary.
[]> secret_words
Do you wish to specify a file for import? [N]>
Enter new words or regular expressions, enter a blank line to finish.
codename
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> settings
Do you want to ignore case when matching using this dictionary? [Y]>
Do you want strings in this dictionary to only match complete words? [Y]>
Enter the default encoding to be used for exporting this dictionary:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[2]>
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]>
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added new dictionary: secret_words

```

```
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

사전 가져오기

아래의 예에서는 **dictionaryconfig** 명령을 사용하여 profanity.txt 텍스트 파일에 있는 84개 용어를 Unicode(UTF-8) 형식으로 profanity라는 사전에 가져옵니다.

```
mail3.example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[ ]> new
Enter a name for this content dictionary.
[ ]> profanity
Do you wish to specify a file for import? [N]> y
Enter the name of the file to import:
[ ]> profanity.txt
Enter the encoding to use for the imported file:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[2]>
84 entries imported successfully.
Currently configured content dictionaries:
1. profanity
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
```

사전 내보내기

아래의 예에서는 **dictionaryconfig** 명령을 사용하여 secret_words 사전을 secret_words_export.txt 라는 텍스트 파일로 내보냅니다.

```
mail3.example.com> dictionaryconfig
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[ ]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[ ]> 1
Choose the operation you want to perform on dictionary 'secret_words':
```



```

- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> export
Enter a name for the exported file:
[]> secret_words_export.txt
mail3.example.com> dictionaryconfig
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> export
Enter a name for the exported file:
[]> secret_words_export.txt

```

exceptionconfig

설명

도메인 예외 테이블을 생성하려면 CLI에서 **exceptionconfig** 명령을 사용합니다. 이 예에서는 이 메일 주소 “admin@zzzaazz.com”이 “Allow”라는 정책의 도메인 예외 테이블에 추가됩니다.

Usage(사용)

Commit: 이 명령은 ‘commit’이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> exceptionconfig
Choose the operation you want to perform:
- NEW - Create a new domain exception table entry
[]> new
Enter a domain, sub-domain, user, or email address for which you wish to
provide an exception:
[]> mail.partner.com
Any of the following passes:

```

```

- @[IP address]
  Matches any email address with this IP address.
- @domain
  Matches any email address with this domain.
- @.partial.domain
  Matches any email address domain ending in this domain.
- user@
  Matches any email address beginning with user@.
- user@domain
  Matches entire email address.
Enter a domain, sub-domain, user, or email address for which you wish to
provide an exception:
[ ]> admin@zzzaazzz.com
Choose a policy for this domain exception:
1. Allow
2. Reject
[1]> 1
Choose the operation you want to perform:
- NEW - Create a new domain exception table entry
- EDIT - Edit a domain exception table entry
- DELETE - Delete a domain exception table entry
- PRINT - Print all domain exception table entries
- SEARCH - Search domain exception table
- CLEAR - Clear all domain exception entries
[ ]>

```

filters

설명

메시지 처리 옵션을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

이 예에서는 filter 명령을 사용하여 3개의 새 필터를 생성합니다.

- 첫 번째 필터 이름은 **big_messages**입니다. 이 필터는 10메가바이트보다 큰 메시지를 삭제하기 위해 **body-size** 규칙을 사용합니다.
- 두 번째 필터의 이름은 **no_mp3s**입니다. 이 필터는 파일 이름 확장명이 **.mp3**인 첨부 파일이 포함된 메시지를 삭제하기 위해 **attachment-filename** 규칙을 사용합니다.
- 세 번째 필터의 이름은 **mailfrompm**입니다. 이 필터는 **postmaster@example.com**의 모든 메일을 검사하고 **administrator@example.com**에 숨은 참조로 보내기 위해 **mail-from** 규칙을 사용합니다.

필터가 활성화되고 유효한지 확인하기 위해 **filter -> list** 하위 명령을 사용하여 필터를 나열한 후 **move** 하위 명령을 사용하여 첫 번째 필터와 마지막 필터의 위치를 전환합니다. 마지막으로, 필터가 적용되도록 변경 사항을 커밋합니다.

```

mail3.example.com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
big_messages:
    if (body-size >= 10M) {
        drop();
    }
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
no_mp3s:
    if (attachment-filename == '\\.mp3$') {
        drop();
    }
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
mailfrompm:
    if (mail-from == "^postmaster$")
        { bcc ("administrator@example.com");}
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

```

policyconfig

설명

수신자 또는 발신자 기반 정책에 따라 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

- 벌크 이메일 또는 소셜 네트워크 이메일로 식별된 메시지를 삭제하는 수신 정책 생성, 234 페이지
- 세일즈 팀을 위한 정책 생성, 218 페이지
- 엔지니어링 팀에 대한 정책 만들기, 220 페이지
- scan_for_confidential 콘텐츠 필터 생성, 222 페이지
- no_mp3s 및 ex_employee 콘텐츠 필터 생성, 225 페이지
- 특정 정책에 대한 콘텐츠 필터 활성화, 229 페이지
- 기본 발신 정책에 대한 DLP 정책, 233 페이지
- 스팸 메시지를 삭제하고 스팸으로 의심되는 메시지를 아카이빙하는 수신 메일 정책 생성, 216 페이지
- AMP 엔진에서 Unscannable(스캔할 수 없음)로 표시된 메시지를 처리하도록 수신 정책 구성, 235 페이지

스팸 메시지를 삭제하고 스팸으로 의심되는 메시지를 아카이빙하는 수신 메일 정책 생성

이 예에서는 `policyconfig -> edit -> antispam` 하위 명령을 사용하여 기본 수신 메일 정책에 대한 안티 스팸 설정을 수정합니다. 이메일 보안 관리자 기능의 GUI에서도 이 동일한 컨피그레이션을 사용할 수 있습니다.

- 먼저 스팸으로 확인된 메시지는 아카이빙에서 제외됩니다. 이 메시지는 삭제됩니다.
- 스팸으로 의심되는 메시지는 아카이빙 대상으로 선택됩니다. 또한 `quarantine.example.com`이라는 서버에 설치된 스팸 격리로 전송됩니다. 텍스트 `[quarantined: possible spam]`이 제목줄의 앞에 추가되고 `X-quarantined: true`라는 특수한 헤더가 이 의심스러운 메시지에 추가되도록 구성됩니다. 이 시나리오에서 관리자와 엔드 유저는 격리에서 오탐을 확인할 수 있으며, 관리자는 필요 시 의심스러운 스팸 임계값을 조정할 수 있습니다.

마지막으로 변경 사항을 커밋합니다.

```
mail3.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 1
Incoming Mail Policy Configuration
```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters

[]> **edit**

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1	DEFAULT	Ironport	Mcafee	N/A	N/A	Off	Enabled

Enter the name or number of the entry you wish to edit:

[]> **1**

Policy Summaries:

Anti-Spam: IronPort - Deliver, Prepend "[SPAM] " to Subject
 Suspect-Spam: IronPort - Deliver, Prepend "[SUSPECTED SPAM] " to Subject
 Anti-Virus: Off

Content Filters: Off (No content filters have been created)

Choose the operation you want to perform:

- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy

[]> **antispm**

Choose the operation you want to perform:

- EDIT - Edit Anti-Spam policy
- DISABLE - Disable Anti-Spam policy (Disables all policy-related actions)

[]> **edit**

Begin Anti-Spam configuration

Some messages will be positively identified as spam. Some messages will be identified as suspected spam. You can set the IronPort Anti-Spam Suspected Spam Threshold below.

The following configuration options apply to messages POSITIVELY identified as spam:

What score would you like to set for the IronPort Anti-Spam spam threshold?

[90]> **90**

1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE

What do you want to do with messages identified as spam?

[1]> **2**

Do you want to archive messages identified as spam? [N]>

Do you want to enable special treatment of suspected spam? [Y]> **y**

What score would you like to set for the IronPort Anti-Spam suspect spam threshold?

[50]> **50**

The following configuration options apply to messages identified as SUSPECTED spam:

1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE

```

What do you want to do with messages identified as SUSPECTED spam?
[1]> 4
Do you want to archive messages identified as SUSPECTED spam? [N]> y
1. PREPEND
2. APPEND
3. NONE
Do you want to add text to the subject of messages identified as SUSPECTED spam?
[1]> 1
What text do you want to prepend to the subject?
[[SUSPECTED SPAM] ]> [quarantined: possible spam]
Do you want to add a custom header to messages identified as SUSPECTED spam? [N]> y
Enter the name of the header:
[> X-quarantined
Enter the text for the content of the header:
[> true
Anti-Spam configuration complete
Policy Summaries:
Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Content Filters: Off (No content filters have been created)
Outbreak Filters: Enabled. No bypass extensions.
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy
[>

```

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
-----	-----	-----	-----	-----	-----	-----
DEFAULT	Ironport	Mcafee	N/A	N/A	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[>
mail3.example.com> commit
Please enter some comments describing your changes:
[> configured anti-spam for Incoming Default Policy
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

세일즈 팀을 위한 정책 생성

Incoming Mail Policy Configuration

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
-----	-----	-----	-----	-----	-----	-----
DEFAULT	Ironport	Mcafee	N/A	N/A	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[ ]> new
Enter the name for this policy:
[ ]> sales_team
Begin entering policy members. The following types of entries are allowed:
Username entries such as joe@, domain entries such as @example.com, sub-domain
entries such as @.example.com, LDAP group memberships such as ldap(Engineers)
Enter a member for this policy:
[ ]> ldap(sales)
Please select an LDAP group query:
1. PublicLDAP.ldapgroup
[1]> 1
Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1
Add another member? [Y]> n
Would you like to enable Anti-Spam support? [Y]> y
Use the policy table default? [Y]> n
Begin Anti-Spam configuration
Some messages will be positively identified as spam. Some messages will be
identified as suspected spam. You can set the IronPort Anti-Spam Suspected Spam Threshold
below.
The following configuration options apply to messages POSITIVELY identified as spam:
What score would you like to set for the IronPort Anti-Spam spam threshold?
[90]> 90
1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as spam?
[1]> 2
Do you want to archive messages identified as spam? [N]> n
Do you want to enable special treatment of suspected spam? [Y]> y
What score would you like to set for the IronPort Anti-Spam suspect spam
threshold?
[50]> 50
The following configuration options apply to messages identified as SUSPECTED
spam:
1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as SUSPECTED spam?
[1]> 4
Do you want to archive messages identified as SUSPECTED spam? [N]> n
1. PREPEND
2. APPEND
3. NONE
Do you want to add text to the subject of messages identified as SUSPECTED
spam?
[1]> 3
Do you want to add a custom header to messages identified as SUSPECTED spam? [N]> n
Anti-Spam configuration complete
Would you like to enable Anti-Virus support? [Y]> y
Use the policy table default? [Y]> y
Would you like to enable Outbreak Filters for this policy? [Y]> y
Use the policy table default? [Y]> y
Incoming Mail Policy Configuration

```

엔지니어링 팀에 대한 정책 만들기

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies

[]>

이제 엔지니어링 팀(개별 이메일 수신자 3명으로 구성됨)을 위한 정책을 생성하여 .dwg 파일이 보안 침해 필터 검사에서 제외되게 합니다.

엔지니어링 팀에 대한 정책 만들기

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies

[]> **new**

Enter the name for this policy:

[]> **engineering**

Begin entering policy members. The following types of entries are allowed:

Username entries such as joe@, domain entries such as @example.com, sub-domain entries such as @.example.com,

LDAP group memberships such as ldap(Engineers)

Enter a member for this policy:

[]> **bob@example.com**

Is this entry a recipient or a sender?

1. Recipient
2. Sender

[1]> **1**


```

Add another member? [Y]> y
Enter a member for this policy:
[]> fred@example.com
Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1
Add another member? [Y]> y
Enter a member for this policy:
[]> joe@example.com
Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1
Add another member? [Y]> n
Would you like to enable Anti-Spam support? [Y]> y
Use the policy table default? [Y]> y
Would you like to enable Anti-Virus support? [Y]> y
Use the policy table default? [Y]> y
Would you like to enable Outbreak Filters for this policy? [Y]> y
Use the policy table default? [Y]> n
Would you like to modify the list of file extensions that bypass
Outbreak Filters? [N]> y
Choose the operation you want to perform:
- NEW - Add a file extension
[]> new
Enter a file extension:
[]> dwg
Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]> print
The following file extensions will bypass Outbreak Filter processing:
dwg
Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]>
Incoming Mail Policy Configuration

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy

```

scan_for_confidential 콘텐츠 필터 생성

```

- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>

```

이제 Incoming Mail Overview(수신 메일 개요) 정책 테이블에서 사용할 3개의 새 콘텐츠 필터를 생성합니다.

CLI에서 policyconfig 명령의 filters 하위 명령은 Incoming Content Filters GUI(수신 콘텐츠 필터 GUI) 페이지와 동일합니다. CLI에서 콘텐츠를 필터를 생성할 때 save 하위 명령을 사용하여 필터를 저장하고 policyconfig 명령으로 돌아옵니다.

먼저 scan_for_confidential 콘텐츠 필터를 생성합니다.

scan_for_confidential 콘텐츠 필터 생성

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

```

- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies

```

```

[]> filters

```

No filters defined.

Choose the operation you want to perform:

```

- NEW - Create a new filter

```

```

[]> new

```

Enter a name for this filter:

```

[]> scan_for_confidential

```

Enter a description or comment for this filter (optional):

```

[]> scan all incoming mail for the string 'confidential'

```

Filter Name: scan_for_confidential

Conditions:

Always Run

Actions:

No actions defined yet.

Description:

```

scan all incoming mail for the string 'confidential'

```

Choose the operation you want to perform:

```

- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[> add
1. Condition
2. Action
[1]> 1
1. Message Body Contains
2. Only Body Contains (Attachments are not scanned)
3. Message Body Size
4. Subject Header
5. Other Header
6. Attachment Contains
7. Attachment File Type
8. Attachment Name
9. Attachment MIME Type
10. Attachment Protected
11. Attachment Unprotected
12. Attachment Corrupt
13. Envelope Recipient Address
14. Envelope Recipient in LDAP Group
15. Envelope Sender Address
16. Envelope Sender in LDAP Group
17. Reputation Score
18. Remote IP
19. DKIM authentication result
20. SPF verification result
[1]> 1
Enter regular expression or smart identifier to search message contents for:
[> confidential
Threshold required for match:
[1]> 1
Filter Name: scan_for_confidential
Conditions:
body-contains("confidential", 1)
Actions:
No actions defined yet.
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry

```

```

17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 1
Enter the email address(es) to send the Bcc message to:
[ ]> hr@example.com
Do you want to edit the subject line used on the Bcc message? [N]> y
Enter the subject to use:
[$Subject]> [message matched confidential filter]
Do you want to edit the return path of the Bcc message? [N]> n
Filter Name: scan_for_confidential
Conditions:
body-contains("confidential", 1)
Actions:
bcc ("hr@example.com", "[message matched confidential filter]")
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[ ]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 14
1. Policy
[1]> 1
Filter Name: scan_for_confidential
Conditions:
body-contains("confidential", 1)
Actions:
bcc ("hr@example.com", "[message matched confidential filter]")
quarantine ("Policy")
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:

```

```

- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- MOVE - Reorder the conditions or actions
- SAVE - Save filter
[]> save
Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- RENAME - Rename a filter
[]>

```

no_mp3s 및 ex_employee 콘텐츠 필터 생성

```

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- RENAME - Rename a filter
[]> new
Enter a name for this filter:
[]> no_mp3s
Enter a description or comment for this filter (optional):
[]> strip all MP3 attachments
Filter Name: no_mp3s
Conditions:
Always Run
Actions:
No actions defined yet.
Description:
strip all MP3 attachments
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)

```

```

19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 12
Enter the file type to strip:
[1]> mp3
Do you want to enter specific text to use in place of any stripped attachments?[N]> n
Filter Name: no_mp3s
Conditions:
Always Run
Actions:
drop-attachments-by-filetype("mp3")
Description:
strip all MP3 attachments
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- SAVE - Save filter
[1]> save
Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter
[1]> new
Enter a name for this filter:
[1]> ex_employee
Enter a description or comment for this filter (optional):
[1]> bounce messages intended for Doug
Filter Name: ex_employee
Conditions:
Always Run
Actions:
No actions defined yet.
Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[1]> add
1. Condition
2. Action
[1]> 1
1. Message Body Contains
2. Only Body Contains (Attachments are not scanned)
3. Message Body Size
4. Subject Header
5. Other Header
6. Attachment Contains
7. Attachment File Type
8. Attachment Name
9. Attachment MIME Type
10. Attachment Protected
11. Attachment Unprotected
12. Attachment Corrupt
13. Envelope Recipient Address

```

```

14. Envelope Recipient in LDAP Group
15. Envelope Sender Address
16. Envelope Sender in LDAP Group
17. Reputation Score
18. Remote IP
19. DKIM authentication result
20. SPF verification result
[1]> 13
Enter regular expression to search Recipient address for:
[]> doug
Filter Name:  ex_employee
Conditions:
rcpt-to == "doug"
Actions:
No actions defined yet.
Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 2
Enter the email address(es) to send the notification to:
[]> joe@example.com
Do you want to edit the subject line used on the notification? [N]> y
Enter the subject to use:
[]> message bounced for ex-employee of example.com
Do you want to edit the return path of the notification? [N]> n
Do you want to include a copy of the original message as an attachment to the
notification? [N]> y
Filter Name:  ex_employee
Conditions:
rcpt-to == "doug"
Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of
example.com")
Description:

```

```

bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 18
Filter Name:  ex_employee
Conditions:
rcpt-to == "doug"
Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of
example.com")
bounce()
Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> save
Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments
3. ex_employee: bounce messages intended for Doug
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter
[]>
Incoming Mail Policy Configuration

```


Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[ ]>

```

특정 정책에 대한 콘텐츠 필터 활성화

아래에서는 일부 정책에 대해서만 콘텐츠 필터를 활성화하기 위해 정책을 다시 활성화하는 방법을 보여 줍니다.

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[ ]> edit

```

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1	sales_team	IronPort	Default	Default	Default	Default	Default
2	engineering	Default	Default	Default	Default	Default	Enabled
3	DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Enter the name or number of the entry you wish to edit:
[]> 3
Policy Summaries:
Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Graymail Detection: Unsubscribe - Disabled
Content Filters: Off
Outbreak Filters: Enabled. No bypass extensions.
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]> filters
Choose the operation you want to perform:
- ENABLE - Enable Content Filters policy
[]> enable
1.      scan_for_confidential
2.      no_mp3s
3.      ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1
1. Active scan_for_confidential
2.      no_mp3s
3.      ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 2
1. Active scan_for_confidential
2. Active no_mp3s
3.      ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3
1. Active scan_for_confidential
2. Active no_mp3s
3. Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>
Policy Summaries:
Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Graymail Detection: Unsubscribe - Disabled
Content Filters: Enabled. Filters: scan_for_confidential, no_mp3s, ex_employee
Outbreak Filters: Enabled. No bypass extensions.
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy

```

- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters

[]>

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Enabled	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies

[]> edit

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1	sales_team	IronPort	Default	Default	Default	Default	Default
2	engineering	Default	Default	Default	Default	Default	Enabled
3	DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Enter the name or number of the entry you wish to edit:

[]> 2

Policy Summaries:

Anti-Spam: Default

Anti-Virus: Default

Graymail Detection: Unsubscribe - Default

Content Filters: Default

Outbreak Filters: Enabled. Bypass extensions: dwg

Choose the operation you want to perform:

- NAME - Change name of policy
- NEW - Add a new member
- DELETE - Remove a member
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy

```

- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]> filters
Choose the operation you want to perform:
- DISABLE - Disable Content Filters policy (Disables all policy-related
actions)
- ENABLE - Enable Content Filters policy
[]> enable
1.      scan_for_confidential
2.      no_mp3s
3.      ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1
1. Active scan_for_confidential
2.      no_mp3s
3.      ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3
1. Active scan_for_confidential
2.      no_mp3s
3. Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>
Policy Summaries:
Anti-Spam: Default
Anti-Virus: Default
Graymail Detection: Unsubscribe - Default
Content Filters: Enabled. Filters: scan_for_confidential, ex_employee
Outbreak Filters: Enabled. Bypass extensions: dwg
Choose the operation you want to perform:
- NAME - Change name of policy
- NEW - Add a new member
- DELETE - Remove a member
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]>
Incoming Mail Policy Configuration

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Enabled	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Enabled	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy

```

```
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```



참고 CLI에는 개별 정책 내에 새 콘텐츠 필터를 추가하는 개념이 없습니다. 그 대신 filters 하위 명령은 반드시 policyconfig 명령의 단일 하위 섹션 내에서 모든 콘텐츠 필터를 관리하게 합니다. 이런 이유로 이 예에서는 drop_large_attachments 추가를 포함하지 않았습니다.

기본 발신 정책에 대한 DLP 정책

여기서는 기본 발신 정책에 DLP 정책을 활성화하는 방법을 보여줍니다.

```
mail3.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 2
Outgoing Mail Policy Configuration
```

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:	DLP:
DEFAULT	N/A	N/A	N/A	Off	Off	Off	Off

```
Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit
```

	Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:	DLP:
1	DEFAULT	N/A	N/A	N/A	Off	Off	Off	Off

```
Enter the name or number of the entry you wish to edit:
[]> 1
Policy Summaries:
Anti-Spam: Off
Anti-Virus: Off
Graymail Detection: Unsubscribe - Disabled
Content Filters: Off (No content filters have been created)
Outbreak Filters: Off
DLP: Off
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
```

별크 이메일 또는 소셜 네트워크 이메일로 식별된 메시지를 삭제하는 수신 정책 생성

```

- DLP - Modify DLP policy
[> dlp
Choose the operation you want to perform:
- ENABLE - Enable DLP policy
[> enable
1. California AB-1298
2. Suspicious Transmission - Zip Files
3. Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[> 1
1. Active California AB-1298
2. Suspicious Transmission - Zip Files
3. Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[> 2
1. Active California AB-1298
2. Active Suspicious Transmission - Zip Files
3. Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[> 3
1. Active California AB-1298
2. Active Suspicious Transmission - Zip Files
3. Active Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[>
Policy Summaries:
Anti-Spam: Off
Anti-Virus: Off
Graymail Detection: Unsubscribe - Disabled
Content Filters: Off (No content filters have been created)
Outbreak Filters: Off
DLP: Enabled. Policies: California AB-1298, Suspicious Transmission - Zip
Files, Restricted Files
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- DLP - Modify DLP policy
[>

```

별크 이메일 또는 소셜 네트워크 이메일로 식별된 메시지를 삭제하는 수신 정책 생성

```

mail.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 1
Incoming Mail Policy Configuration

```

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
DEFAULT	Off	N/A	N/A	Off	Off	N/A

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies

```

```
- FILTERS - Edit content filters
[ ]> edit
```

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1.	DEFAULT	Off	N/A	N/A	Off	Off	N/A

```
Enter the name or number of the entry you wish to edit:
```

```
[ ]> 1
```

```
Policy Summaries:
```

```
Anti-Spam: Off
```

```
Graymail Detection: Off
```

```
Content Filters: Off (No content filters have been created)
```

```
Choose the operation you want to perform:
```

```
- ANTISPAM - Modify Anti-Spam policy
```

```
- GRAYMAIL - Modify Graymail policy
```

```
- FILTERS - Modify filters
```

```
[ ]> graymail
```

```
Choose the operation you want to perform:
```

```
- ENABLE - Enable Graymail policy
```

```
[ ]> enable
```

```
Begin Graymail configuration
```

```
Do you want to enable Safe Unsubscribe? [N]> y
```

```
Do you want to perform Safe Unsubscribe action only for unsigned messages (recommended)?
```

```
[Y]>
```

```
Do you want to enable actions on messages identified as Marketing Email? [N]>
```

```
Do you want to enable actions on messages identified as Social Networking Email? [N]> y
```

```
1. DELIVER
```

```
2. DROP
```

```
3. BOUNCE
```

```
What do you want to do with messages identified as Social Networking Email?
```

```
[1]> 2
```

```
Do you want to archive messages identified as Social Networking Email? [N]>
```

```
Do you want to enable actions on messages identified as Bulk Email? [N]> y
```

```
1. DELIVER
```

```
2. DROP
```

```
3. BOUNCE
```

```
What do you want to do with messages identified as Bulk Email?
```

```
[1]> 2
```

```
Do you want to archive messages identified as Bulk Email? [N]>
```

```
Graymail configuration complete.
```

```
Policy Summaries:
```

```
Anti-Spam: Off
```

```
Graymail Detection: Unsubscribe - Enabled
```

```
    Social Networking mails : Drop
```

```
    Bulk mails : Drop
```

```
Content Filters: Off (No content filters have been created)
```

```
Choose the operation you want to perform:
```

```
- ANTISPAM - Modify Anti-Spam policy
```

```
- GRAYMAIL - Modify Graymail policy
```

```
- FILTERS - Modify filters
```

```
[ ]>
```

AMP 엔진에서 **Unscannable**(스캔할 수 없음)로 표시된 메시지를 처리하도록 수신 정책 구성

```
mail.example.com> policyconfig
```

```
Would you like to configure Incoming or Outgoing Mail Policies?
```

```
1. Incoming
```

```
2. Outgoing
[1]> 1
Incoming Mail Policy Configuration
```

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
DEFAULT	Off	N/A	N/A	Off	Off	N/A

```
Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit
```

	Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
1.	DEFAULT	Off	N/A	N/A	Off	Off	N/A

```
Enter the name or number of the entry you wish to edit:
[]> 1
```

```
Policy Summaries:
```

```
Advanced Malware Protection: Malware Action - drop , Message Error Unscannable Action - deliver , Rate Limit Unscannable Action - deliver , AMP Service Not Available Unscannable Action - deliver , File Analysis Action - Deliver , Mailbox Auto Remediation (MAR) - Disabled
Content Filters: Off
Outbreak Filters: Off
```

```
Choose the operation you want to perform:
- OUTBREAK - Modify Outbreak Filters policy
- ADVANCEDMALWARE - Modify Advanced Malware Protection policy
- FILTERS - Modify filters
[]> advancedmalware
```

```
Choose the operation you want to perform:
- EDIT - Edit Advanced-Malware protection policy
- DISABLE - Disable Advanced-Malware protection policy (Disables all policy-related actions)
[]> edit
```

```
Begin AMP configuration
```

```
Do you want to enable File Analysis? [Y]>
```

```
Do you like the system to automatically insert an X-header with the anti-malware scanning results? (Recommended for trouble-shooting) [Y]>
```

```
Unscannable Message Handling
```

```
Current actions to take if any of the attachments could not be scanned due to message errors:
```

- WARNING: Delivering Unscannable due to Message Errors messages normally
- Prepending subjects with "[WARNING: ATTACHMENT UNSCANNED]"
- Archiving copies of the original message.


```

Do you want to edit the actions for Unscannable Message due to message errors? [N]> yes

Current actions to take if any of the attachments could not be scanned due to rate limit hit:
- WARNING: Delivering Unscannable due to Rate Limit messages normally
- Prepending subjects with "[WARNING: ATTACHMENT UNSCANNED]"
- Archiving copies of the original message.
Do you want to edit the actions for Unscannable Message due to rate limit hit? [N]> yes

Current actions to take if any of the attachments could not be scanned due to AMP Service not available:
- WARNING: Delivering Unscannable due to AMP Service Not Available messages normally
- Prepending subjects with "[WARNING: ATTACHMENT UNSCANNED]"
- Archiving copies of the original message.
Do you want to edit the actions for Unscannable Message due to AMP Service not available? [N]> yes

```

예: "From(보낸 사람)" 헤더에 대한 우선순위 설정

다음 예에서는 `policyconfig > match headers priority sub` 명령을 사용하여 어플라이언스의 수신 및 발신 메시지와 일치하도록 "From" 메시지 헤더의 우선순위를 설정합니다.

```

mail1.example.com > policyconfig

Would you like to configure Incoming Mail Policy or Outgoing Mail Policies or Match Headers Priority?

1. Incoming Mail Policies
2. Outgoing Mail Policies
3. Match Headers Priority
[1]> 3

Match Headers Priority Configuration
Priority:      Headers:
-----      -
P1           Envelope Sender

Choose the operation you want to perform:
- ADD - Add match priority for headers
- EDIT - Edit an existing match priority for headers
- REMOVE - Remove an existing match priority for headers
[]> add

Choose headers for priority 2
Add header "From" Header:
1. Yes
2. No
[1]> 1

Add header "Reply-To" Header:
1. Yes
2. No
[1]> 2

Add header "Sender" Header:
1. Yes
2. No
[1]> 2

Match Headers Priority Configuration
Priority:      Headers:
-----      -

```

```
P1      Envelope Sender
P2      "From" Header
```

quarantineconfig

설명

시스템 격리를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> quarantineconfig
Currently configured quarantines:
# Quarantine Name      Size (MB) % full  Messages  Retention  Policy
1  Outbreak            3,072    0.0      1          12h       Release
2  Policy               1,024    0.1      497        10d       Delete
3  Virus                2,048    empty    0          30d       Delete
2,048 MB available for quarantine allocation.
Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- OUTBREAKMANAGE - Manage the Outbreak Filters quarantine.
[ ]> new
Please enter the name for this quarantine:
[ ]> HRQuarantine
Retention period for this quarantine. (Use 'd' for days or 'h' for hours or 'm' for
'minutes'.):
[ ]> 15d
1. Delete
2. Release
Enter default action for quarantine:
[1]> 2
Do you want to modify the subject of messages that are released because
"HRQuarantine" overflows? [N]>
Do you want add a custom header to messages that are released because
"HRQuarantine" overflows? [N]>
Do you want to strip all attachments from messages that are released
because "HRQuarantine" overflows? [N]>
Do you want default action to apply automatically when quarantine space fills up? [Y]>
Currently configured quarantines:
# Quarantine Name      Size (MB) % full  Messages  Retention  Policy
1  HRQuarantine         1,024    N/A      N/A        15d       Release
2  Outbreak            3,072    0.0      1          12h       Release
3  Policy               1,024    0.1      497        10d       Delete
4  Virus                2,048    empty    0          30d       Delete
(N/A: Quarantine contents is not available at this time.)
1,024 MB available for quarantine allocation.
Choose the operation you want to perform:
```

- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- OUTBREAKMANAGE - Manage the Outbreak Filters quarantine.

사용자와 격리

사용자를 추가할지 묻는 질문에 “y” 또는 yes라고 답하면 사용자 관리를 시작합니다. 여기서 사용자 목록을 관리할 수 있습니다. 다른 격리 컨피그레이션 질문을 거칠 필요 없이 격리에 여러 사용자를 추가하거나 삭제할 수 있습니다. 빈 프롬프트([]>)에서 Return(Enter)을 입력하여 사용자 관리 섹션을 종료하고 계속 격리를 구성합니다.



참고 게스트 또는 운영자 사용자가 이미 시스템에서 생성된 경우 사용자에게 격리에 대한 액세스 권한을 부여하는 프롬프트만 나타납니다.

격리의 사용자 이름은 운영자 또는 게스트 그룹에 속한 사용자만 포함합니다. 관리자 그룹의 사용자는 항상 격리에 대한 완전한 액세스 권한을 갖습니다. 사용자 목록을 관리할 때 모든 운영자/게스트 사용자가 이미 격리의 사용자 목록에 있다면 NEW 명령은 사용할 수 없습니다. 마찬가지로 삭제할 사용자가 없을 경우 DELETE를 사용할 수 없습니다.

scanconfig

설명

첨부 파일 검사 정책을 구성합니다.

Usage(사용)

Commit: 이 명령은 ‘commit’이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

예

이 예에서 scanconfig 명령은 다음 매개변수를 설정합니다.

- video/*, audio/*, image/*의 MIME 유형은 건너뛴니다(콘텐츠 검사하지 않음).
- 중첩(재귀) 아카이브 첨부 파일은 최대 10레벨까지 검사합니다. 기본값은 5레벨입니다.
- 검사할 첨부 파일의 최대 크기는 25MB로, 이보다 큰 파일은 건너뛴니다. (기본값은 5MB입니다.)
- 문서 메타데이터는 검사합니다.
- 첨부 파일 검사 시간 초과는 180초로 설정됩니다.
- 검사하지 않은 첨부 파일은 검색 패턴과 매치하지 않는 것으로 가정합니다. 이는 기본 동작입니다.
- 일반 본문 텍스트 또는 MIME 유형이 plain/text이거나 plain/html인 텍스트에 대해 아무것도 지정되지 않을 경우 ASCII 인코딩이 사용되도록 구성되었습니다.



참고

assume the attachment matches the search pattern을 Y로 설정할 경우, 검사할 수 없는 메시지에 메시지 필터 규칙을 적용하면 True가 됩니다. 이로 인해 사전과 일치하지 않는 메시지 격리와 같이 예기치 않은 동작이 발생하게 되지만 콘텐츠를 올바르게 검사할 수 없기 때문에 격리됩니다. 이 설정은 DLP 스캐닝에는 적용되지 않습니다.

```
mail3.example.com> scanconfig
There are currently 5 attachment type mappings configured to be SKIPPED.
Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[1]> setup
1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.
Choose one:
[2]> 2
Enter the maximum depth of attachment recursion to scan:
[5]> 10
Enter the maximum size of attachment to scan:
[5242880]> 10m
Do you want to scan attachment metadata? [Y]> y
Enter the attachment scanning timeout (in seconds):
[30]> 180
If a message has attachments that were not scanned for any reason (e.g.
because of size, depth limits, or scanning timeout), assume the attachment matches the
search pattern? [N]> n
If a message could not be deconstructed into its component parts in order to remove specified
attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[1]>
Configure encoding to use when none is specified for plain body text or
anything with MIME type plain/text or plain/html.
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[1]> 1
Scan behavior changed.
There are currently 5 attachment type mappings configured to be SKIPPED.
Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
```

```

- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[]> print
1. Fingerprint      Image
2. Fingerprint      Media
3. MIME Type        audio/*
4. MIME Type        image/*
5. MIME Type        video/*

```

예: 스캔할 수 없는 메시지에 대한 메시지 처리 작업 구성

다음 예에서는 `scanconfig > setup` 명령을 사용하여 첨부 파일 추출 실패로 인해 콘텐츠 스캐너에서 스캔되지 않은 메시지에 대한 메시지 처리 작업을 활성화하고 구성합니다.

```

mail3.example.com> scanconfig
There are currently 5 attachment type mappings configured to be SKIPPED. Choose the operation
you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
-[]>SMIMEsetup- Configure S/MIME unpacking.
[] > setup

1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.

Choose one: [2]>

Enter the maximum depth of attachment recursion to scan: [5]>

Enter the maximum size of attachment to scan: [5242880]>

Do you want to scan attachment metadata? [Y]>

Enter the attachment scanning timeout (in seconds): [30]>

If a message has attachments that were not scanned for any reason (e.g.
because of size, depth limits, or scanning timeout), assume the attachment matches the
search pattern? [N]>

In case of a content or message filter error, should all filters be bypassed? [Y]>

Assume zip file to be unscannable if files in the archive cannot be read? [0]>

If a message could not be deconstructed into its component parts in order
to remove specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[1]>

Configure encoding to use when none is specified for
plain body text or anything with MIME type plain/text or plain/html.

1. US-ASCII

```

```

2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)

[ ]> Do you want to enable actions on unscannable messages due to an extraction failure? y/n
[ Y ]> Yes

1. Drop Message
2. Deliver As Is
3. Quarantine

Action applied to original message: [2]> 2

Do you want to deliver mail to an alternate mailhost ? [N]> yes

Enter the mailhost to deliver to: [ ]> mail.example.com

Do you want to redirect mail to an alternate email address ? [N]> yes

Enter the address to deliver to:
[ ]> user@mail.example.com

Do you want to add a custom header? [N]> yes

Enter the header name: [ ]> Unscannable Messages

Enter the header content:
[ ]> Actions taken on Unscannable Messages

Do you want to modify the subject? [N]> yes

1. Prepend
2. Append

Select position of text: [1]> 1

Enter the text to add:
[[WARNING: UNSCANNABLE EXTRACTION FAILED]]> [WARNING: UNSCANNABLE FILE EXTRACTION FAILURE]

```

stripheaders

설명

제거할 메시지 헤더의 목록을 정의합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> stripheaders
Not currently stripping any headers.
Choose the operation you want to perform:
- SETUP - Set message headers to remove.
[]> setup
Enter the list of headers you wish to strip from the messages before they are delivered.
Separate multiple headers with commas.
[]> Delivered-To
Currently stripping headers: Delivered-To
Choose the operation you want to perform:
- SETUP - Set message headers to remove.
[]>
mail3.example.com>
```

textconfig

설명

안티바이러스 알림 템플릿, 메시지 면책 조항, 알림 템플릿(예: DLP, 바운스, 암호화 알림) 등의 텍스트 리소스를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

텍스트 리소스를 생성하려면 **textconfig -> NEW**를, 삭제하려면 **textconfig > delete**를 사용합니다.

```
mail3.example.com> textconfig
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[]> new
What kind of text resource would you like to create?
1. Anti-Virus Container Template
2. Anti-Virus Notification Template
3. DLP Notification Template
4. Bounce and Encryption Failure Notification Template
5. Message Disclaimer
6. Encryption Notification Template (HTML)
7. Encryption Notification Template (text)
8. Notification Template
[1]> 5
Please create a name for the message disclaimer:
[]> disclaimer 1
```

```

Enter the encoding for the message disclaimer:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[1]>
Enter or paste the message disclaimer here. Enter '.' on a blank line to end.
This message was sent from an IronPort(tm) Email Security appliance.
.
Message disclaimer "disclaimer 1" created.
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[ ]> delete
Please enter the name or number of the resource to delete:
[ ]> 1
Message disclaimer "disclaimer 1" has been deleted.
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[ ]>

```

기존 텍스트 리소스를 수정하려면 **textconfig -> EDIT**를 사용합니다. 인코딩을 변경하거나 선택한 텍스트 리소스의 텍스트를 대체할 수 있습니다.

텍스트 리소스 가져오기

텍스트 파일을 텍스트 리소스로 가져오려면 **textconfig -> IMPORT**를 사용합니다. 텍스트 파일이 어플라이언스의 컨피그레이션 디렉터리에 있어야 합니다.

```

mail3.example.com> textconfig
Current Text Resources:
1. footer.2.message (Message Footer)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[ ]> import
What kind of text resource would you like to create?
1. Anti-Virus Container Template
2. Anti-Virus Notification Template
3. DLP Notification Template
4. Bounce and Encryption Failure Notification Template

```



```

5. Message Disclaimer
6. Encryption Notification Template (HTML)
7. Encryption Notification Template (text)
8. Notification Template
[1]> 8
Please create a name for the notification template:
[]> strip.mp3files
Enter the name of the file to import:
[]> strip.mp3.txt
Enter the encoding to use for the imported file:
1. US-ASCII
[ list of encodings ]
[1]>
Notification template "strip.mp3files" created.
Current Text Resources:
1. disclaimer.2.message (Message Disclaimer)
2. strip.mp3files (Notification Template)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>

```

텍스트 리소스 내보내기

텍스트 리소스를 텍스트 파일로 내보내려면 **textconfig** -> **EXPORT**를 사용합니다. 텍스트 파일이 어플라이언스의 컨피그레이션 디렉터리에 생성됩니다.

```

mail3.example.com> textconfig
Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> export
Please enter the name or number of the resource to export:
[]> 2
Enter the name of the file to export:
[strip.mp3]> strip.mp3.txt
Enter the encoding to use for the exported file:
1. US-ASCII
[ list of encoding types ]
[1]>
File written on machine "mail3.example.com" using us-ascii encoding.
Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.

```

```
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>
```

로깅 및 알림

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [alertconfig, 246 페이지](#)
- [displayalerts, 247 페이지](#)
- [findevent, 248 페이지](#)
- [grep, 250 페이지](#)
- [logconfig, 251 페이지](#)
- [rollovernow, 257 페이지](#)
- [snmpconfig, 258 페이지](#)
- [tail, 260 페이지](#)

alertconfig

설명

이메일 알림을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예: 새 알림 생성

이 예에서는 새 알림 수신자(alertadmin@example.com)를 생성하고 중요 시스템, 하드웨어, 디렉터리 수집 공격 알림을 수신하도록 설정합니다.

```
vm30esa0086.ibqa> alertconfig
Not sending alerts (no configured addresses)
Alerts will be sent using the system-default From Address.
Cisco IronPort AutoSupport: Disabled
Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> new
Please enter a new email address to send alerts.
(Ex: "administrator@example.com")
[]> alertadmin@example.com
Choose the Alert Classes. Separate multiple choices with commas.
```

```

1. All
2. System
3. Hardware
4. Updater
5. Outbreak Filters
6. Anti-Virus
7. Anti-Spam
8. Directory Harvest Attack Prevention
9. Release and Support Notifications
[1]> 2,3,8
Select a Severity Level. Separate multiple choices with commas.
1. All
2. Critical
3. Warning
4. Information
[1]> 2
Sending alerts to:
  alertadmin@example.com
      Class: Hardware - Severities: Critical
      Class: Directory Harvest Attack Prevention - Severities: Critical
      Class: System - Severities: Critical
Initial number of seconds to wait before sending a duplicate alert: 300
Maximum number of seconds to wait before sending a duplicate alert: 3600
Maximum number of alerts stored in the system are: 50
Alerts will be sent using the system-default From Address.
Cisco IronPort AutoSupport: Disabled
Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify alert subscription for an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[ ]>

```

displayalerts

설명

어플라이언스에서 마지막으로 전송된 n개의 알림을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

> displayalerts
Date and Time Stamp          Description
-----
10 Mar 2015 11:33:36 +0000    The updater could not validate the server certificate. Server
certificate not validated - unable to get local issuer
certificate
Last message occurred 28 times between Tue Mar 10 10:34:57 2015 and Tue Mar 10 11:32:24

```

```

2015.
10 Mar 2015 11:23:39 +0000    The updater has been unable to communicate with the update
server for at least 1h.
Last message occurred 8 times between Tue Mar 10 10:29:57 2015 and Tue Mar 10 11:18:24 2015.
10 Mar 2015 10:33:36 +0000    The updater could not validate the server certificate.  Server
certificate not validated - unable to get local issuer
certificate
Last message occurred 26 times between Tue Mar 10 09:33:55 2015 and Tue Mar 10 10:29:57
2015.
10 Mar 2015 10:23:39 +0000    The updater has been unable to communicate with the update
server for at least 1h.
Last message occurred 9 times between Tue Mar 10 09:26:54 2015 and Tue Mar 10 10:22:56 2015.

```

findevent

설명

메일 로그 파일에서 이벤트를 찾습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예: envelope FROM 기준 검색

```

mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 1
Enter the regular expression to search for.
[1]> "
Currently configured logs:
  Log Name          Log Type          Retrieval          Interval
-----
1. mail_logs       IronPort Text Mail Logs  Manual Download    None
Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
No matching message IDs were found

```

예: 메시지 ID 기준 검색

```

mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM

```

```

2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 2
Enter the Message ID (MID) to search for.
[]> 1
Currently configured logs:
-----
      Log Name          Log Type          Retrieval          Interval
-----
  1. mail_logs          IronPort Text Mail Logs      Manual Download      None
Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 1

```

예: 제목 기준 검색

```

mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 3
Enter the regular expression to search for.
[]> "
Currently configured logs:
-----
      Log Name          Log Type          Retrieval          Interval
-----
  1. mail_logs          IronPort Text Mail Logs      Manual Download      None
Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 2
Available mail log files, listed by log file start time.
Specify multiple log files by separating with commas or specify a range with a dash:
1. Thu Feb 19 05:18:02 2015
[1]>
No matching message IDs were found

```

예: envelope TO 기준 검색

```

mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 4
Enter the regular expression to search for.
[]> '
Currently configured logs:
-----
      Log Name          Log Type          Retrieval          Interval
-----
  1. mail_logs          IronPort Text Mail Logs      Manual Download      None

```

```

Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
No matching message IDs were found

```

grep

설명

로그 파일에서 텍스트를 검색합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

grep 명령을 사용하여 로그 내에서 텍스트 문자열을 검색할 수 있습니다. grep 명령을 실행하려면 다음 구문을 사용합니다.

```
grep [-C count] [-e regex] [-i] [-p] [-t] [regex] log_name
```



참고 -e regex 또는 regex를 입력해야 결과를 반환합니다.

grep 명령을 실행하려면 다음 옵션을 사용합니다.

표 11: grep 명령 옵션

옵션	설명
-C	찾은 grep 패턴 주변의 컨텍스트 라인을 제공합니다. 포함할 라인 수를 지정하려면 값을 입력합니다.
-e	정규 표현식을 입력합니다.
-i	대/소문자를 구분하지 않습니다.
-p	출력에서 페이지를 매깁니다.
-t	로그 파일의 tail에 대해 grep 명령을 실행합니다.

옵션	설명
regex	정규 표현식을 입력합니다.

grep의 예

다음 예에서는 안티바이러스 로그 내에서 텍스트 문자열 'clean' 또는 'viral'을 검색하는 것을 보여줍니다. **grep** 명령은 regex 식을 포함합니다.

```
mail3.example.com> grep "CLEAN\\|VIRAL" antivirus
Fri Jun 9 21:50:25 2006 Info: sophos antivirus - MID 1 - Result 'CLEAN' ()
Fri Jun 9 21:53:15 2006 Info: sophos antivirus - MID 2 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 3 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 4 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 5 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 6 - Result 'CLEAN' ()
Fri Jun 9 22:47:42 2006 Info: sophos antivirus - MID 12 - Result 'CLEAN' ()
Fri Jun 9 22:53:04 2006 Info: sophos antivirus - MID 18 - Result 'VIRAL' ()
Fri Jun 9 22:53:05 2006 Info: sophos antivirus - MID 16 - Result 'VIRAL' ()
Fri Jun 9 22:53:06 2006 Info: sophos antivirus - MID 19 - Result 'VIRAL' ()
Fri Jun 9 22:53:07 2006 Info: sophos antivirus - MID 21 - Result 'VIRAL' ()
Fri Jun 9 22:53:08 2006 Info: sophos antivirus - MID 20 - Result 'VIRAL' ()
Fri Jun 9 22:53:08 2006 Info: sophos antivirus - MID 22 - Result 'VIRAL' ()
mail3.example.com>
```

logconfig

설명

로그 파일에 대한 액세스를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

FTP 푸시 로그 서브스크립션의 예

다음 예에서는 **logconfig** 명령을 사용하여 myDeliveryLogs라는 새 전달 로그를 구성합니다. 그런 다음 로그가 FTP를 통해 원격 호스트에 푸시되도록 구성합니다.

```
mail3.example.com> logconfig
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
```

```

8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[1]> new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs
[1]> 8
Please enter the name for the log:
[1]> myDeliveryLogs
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> 2
Hostname to deliver the logs:
[1]> yourhost.example.com
Username on the remote host:

```



```
[ ]> yourusername
Passphrase for your user:
[ ]> thepassphrase
Directory on remote host to place logs:
[ ]> /logs
Filename to use for log files:
[conversation.text]>
Maximum time to wait before transferring:
[3600]>
Maximum filesize before transferring:
[10485760]>
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "myDeliveryLogs" Type: "SMTP Conversation Logs" Retrieval: FTP Push - Host
yourhost.example.com
16. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
17. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
18. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
19. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
20. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
21. "status" Type: "Status Logs" Retrieval: FTP Poll
22. "system_logs" Type: "System Logs" Retrieval: FTP Poll
23. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
24. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
```

SCP 푸시 로그 서브스크립션의 예

다음 예에서는 **logconfig** 명령을 사용하여 LogPush라는 새 전달 로그를 구성합니다. 이 로그는 SCP를 통해 IP 주소가 10.1.1.1인 원격 호스트에 사용자 **logger**로 푸시되어 디렉터리 **/tmp**에 저장되도록 구성됩니다. 로그 검색 방법이 SCP 푸시일 경우 **sshconfig** 명령이 **logconfig** 명령 내에서 자동으로 호출됩니다. 호스트 키 및 사용자 키에 대한 자세한 내용은 각각 *AsyncOS for Cisco Email Security Appliances* 사용자 가이드에서 "호스트 키 구성" 및 "SSH 키 관리"를 참고하십시오. 또한 IP 주소를 호스트 이름 프로토타프로 사용할 수 있습니다.

```
mail3.example.com> logconfig
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
```

```

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "sblld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[> new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs
[1]> 3
Please enter the name for the log:
[> LogPush
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 3
Hostname to deliver the logs:
[> 10.1.1.1
Port to connect to on the remote host:
[22]>
Username on the remote host:
[> logger
Directory on remote host to place logs:
[> /tmp

```

```

Filename to use for log files:
[delivery.log]>
Maximum time to wait before transferring:
[3600]>
Maximum filesize before transferring:
[10485760]>
Protocol:
1. SSH1
2. SSH2
[2]> 2
Do you want to enable host key checking? [N]> y
Do you want to automatically scan the host for its SSH key, or enter it
manually?
1. Automatically scan.
2. Enter manually.
[1]> 1
SSH2:dsa
10.1.1.1 ssh-dss
AAAAB3NzaC1kc3MAAACBALwGi4I1WLDVndbIwEsArt9LVE2ts5yE9JBTSdUwLvoq0G3FRqifrc92zgyHtc/
ZWYxavUTIM3XdlbpiEcscMp2XKpSnPPx2ly8bqkpsJSQCcm8zZMDjnOPm8ghiwHXYh7oNEUJCCPNpxAy44r1J5Yz4x9eIoAlp0dHU0GR
+j1NAAAAFQDQi5GY/X9P1DM3fPMvEx7wc0edlwAAAIB9cgMTEFP1WTAGrlRtbowZP5zWZtVDTxLhdXzjlo4+bB4hBR7DKuc80+naAFnThyH/
J8R3WLJVF79M5geK1bXzuJGDK3ZwL3UYefPcBqXp20LzLQCSJyx1WrwYz/rooqN1EnF4sh12mtq3tde1176bQgtwaQA4wKOL5k3zOWsPwAAAIaICRYat3y+Blv/
V6wDEBBk+oULv3eK38gaFuip4WMBxkG9G06EQi8nss82oznwBy/pITRQfh4MBmlxTF4VEY00sArR1ZtuUJC1QQQvCgh7Nd3YNais2CSbEKEEaIOTf6+
SX2RNpcUF3Wg5yggw92xtqQPKMcZeLTK2ZJRkhC+Vw==
Add the preceding host key(s) for 10.1.1.1? [Y]> y
Currently installed host keys:
1. 10.1.1.1 1024 35 12260642076447444117847407996206675325...3520565607
2. 10.1.1.1 ssh-dss AAAAB3NzaC1kc3MAAACBALwGi4I1WLDVndbIwE...JRkhC+Vw==
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display this machine's host keys.
[ ]>
Maximum filesize before transferring:
[10485760]>
Protocol:
1. SSH1
2. SSH2
[2]> 2
Do you want to enable host key checking? [N]> y
Currently installed host keys:
Choose the operation you want to perform:
- NEW - Add a new key.
- SCAN - Automatically download a host key.
- HOST - Display this machine's host keys.
[ ]> scan
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]> 4
SSH1:rsa
10.1.1.1 1024 35
122606420764474441178474079962066753259278682648965870690129496065430424463013457294798980627829828033793152226
44869451431621827281445398693161250828232800881574007210997563235647853212881618780683074632823432777810013112817667266624451119
1783747965898000855947022484692079466697707373948871554575173520565607

```

Syslog 푸시 로그 서브스크립션의 예

다음 예에서는 **logconfig** 명령을 사용하여 MailLogSyslogPush라는 새 전달 로그를 구성합니다. 이 로그는 UPD와 'mail' 기능을 사용하여 IP 주소가 10.1.1.2인 원격 syslog 서버에 푸시되고 디렉터리에 저장되도록 구성됩니다.

```
mail3.example.com> logconfig
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[ ]> new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
```

```

23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs
[1]> 1
Please enter the name for the log:
[]> MailLogSyslogPush
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 2
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> 4
Hostname to deliver the logs:
[]> 10.1.1.2
Which protocol do you want to use to transfer the log data?
1. UDP
2. TCP
[1]> 1
Which facility do you want the log data to be sent as?
1. auth
2. authpriv
3. console
4. daemon
5. ftp
6. local0
7. local1
8. local2
9. local3
10. local4
11. local5
12. local6
13. local7
14. mail
15. ntp
16. security
17. user
[14]> 14
Currently configured logs:
1. "MailLogSyslogPush" Type: "IronPort Text Mail Logs" Retrieval: Syslog Push -
Host 10.1.1.2

```

rollovernow

설명

로그 파일을 롤오버합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> rollovernow
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "sblld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
24. All Logs
Which log would you like to roll over?
[]> 2
Log files successfully rolled over.
mail3.example.com>
```

snmpconfig

설명

SNMP를 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 snmpconfig 명령을 사용하여 포트 161의 "PublicNet" 인터페이스에서 SNMP를 활성화합니다. 버전 3의 패스프레이즈를 입력하고 확인을 위해 다시 입력합니다. 시스템이 버전 1과 버전 2 요청을 처리하도록 구성되고 버전 1과 버전 2의 GET 요청을 위해 커뮤니티 문자열 public이 입력됩니

다. 트랩 대상 `snmp-monitor.example.com`이 입력됩니다. 마지막으로, 시스템 위치 및 연락처 정보가 입력됩니다.

```
mail3.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> setup
Do you want to enable SNMP? [N]> y
Please choose an IP interface for SNMP requests.
1. Data 1 (192.168.1.1/24: buttercup.run)
2. Data 2 (192.168.2.1/24: buttercup.run)
3. Management (192.168.44.44/24: buttercup.run)
[1]>
Enter the SNMPv3 passphrase.
>
Please enter the SNMPv3 passphrase again to confirm.
>
Which port shall the SNMP daemon listen on?
[161]>
Service SNMP V1/V2c requests? [N]> y
Enter the SNMP V1/V2c community string.
[]> public
From which network shall SNMP V1/V2c requests be allowed?
[192.168.2.0/24]>
Enter the Trap target (IP address). Enter "None" to disable traps.
[None]> snmp-monitor.example.com
Enterprise Trap Status
1. RAIDStatusChange           Enabled
2. fanFailure                  Enabled
3. highTemperature             Enabled
4. keyExpiration               Enabled
5. linkDown                    Enabled
6. linkUp                      Enabled
7. powerSupplyStatusChange     Enabled
8. resourceConservationMode     Enabled
9. updateFailure               Enabled
Do you want to change any of these settings? [N]> y
Do you want to disable any of these traps? [Y]>
Enter number or numbers of traps to disable. Separate multiple numbers with commas.
[]> 1,8
Enterprise Trap Status
1. RAIDStatusChange           Disabled
2. fanFailure                  Enabled
3. highTemperature             Enabled
4. keyExpiration               Enabled
5. linkDown                    Enabled
6. linkUp                      Enabled
7. powerSupplyStatusChange     Enabled
8. resourceConservationMode     Disabled
9. updateFailure               Enabled
Do you want to change any of these settings? [N]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #31, position 2
Enter the System Contact string.
[snmp@localhost]> Joe Administrator, x8888
Current SNMP settings:
Listening on interface "Data 1" 192.168.2.1/24 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.
SNMP v1/v2 Community String: public
```

```

Trap target: snmp-monitor.example.com
Location: Network Operations Center - west; rack #31, position 2
System Contact: Joe Administrator, x8888
mail3.example.com>

```

tail

설명

지속적으로 로그 파일의 끝을 표시합니다. 또한 **tail** 명령은 표시할 로그의 이름 또는 번호를 매개변수 **tail 9** 또는 **tail mail_logs**로 받습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> tail
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 19
Press Ctrl-C to stop.
Sat May 15 12:25:10 2008 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host
Sat May 15 23:18:10 2008 Info: PID 19626: User admin commit changes:
Sat May 15 23:18:10 2008 Info: PID 274: User system commit changes: Updated filter logs
config
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Receiving suspended.

```



```
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Suspended receiving.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving resumed.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving resumed.
Sat May 15 23:48:17 2008 Info: PID 25696: User admin commit changes:
Sun May 16 00:00:00 2008 Info: Generated report: name b, start time Sun May 16 00:00:00
2004, size 2154 bytes
^C
mail3.example.com>
```

보고

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [reportingconfig, 261 페이지](#)

reportingconfig

reportingconfig 명령 사용

reportingconfig 하위 메뉴에서 다음 하위 명령을 사용할 수 있습니다.

표 12: reportingconfig 하위 명령

Syntax	설명	사용 가능
filters	Security Management Appliance를 위한 필터를 구성합니다.	M Series만
alert_timeout	보고 데이터를 받지 못했다는 알림이 표시 될 때를 구성합니다.	M Series만
domain	도메인 보고서 설정을 구성합니다.	M Series만
mode	Security Management Appliance에서 중앙 집중식 보고를 활성화합니다. Email Security Appliance에 대한 중앙 집중식 또는 로컬 보고를 활성화합니다.	C Series, M Series
mailsetup	Email Security Appliance에 대한 보고를 구성합니다.	C Series만

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

예: 보고 필터 활성화(M Series만)

```
mail3.example.com> reportingconfig
Choose the operation you want to perform:
```

```

- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[> filters
Filters remove specific sets of centralized reporting data from the "last year" reports.
Data from the reporting groups selected below will not be recorded.
All filtering has been disabled.
1. No Filtering enabled
2. IP Connection Level Detail.
3. User Detail.
4. Mail Traffic Detail.
Choose which groups to filter, you can specify multiple filters by entering a comma separated
list:
[> 2, 3
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get
reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[>

```

도메인 보고서에 대한 HAT REJECT 정보 활성화(M Series만)

```

mail3.example.com> reportingconfig
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[> domain
If you have configured HAT REJECT policy on all remote appliances providing reporting data
to this appliance to occur at the message
recipient level then of domain reports.
Use message recipient HAT REJECT information for domain reports? [N]> y
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[>

```

시간 초과 알림 활성화(M Series만)

```

mail3.example.com> reportingconfig
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[> alert_timeout
An alert will be sent if reporting data has not been fetched from an appliance after 360
minutes.
Would you like timeout alerts to be enabled? [Y]> y
After how many minutes should an alert be sent?
[360]> 240
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.

```

```
- MODE - Enable/disable centralized reporting.
[]>
```

Email Security Appliance에 대한 중앙 집중식 보고 활성화

```
mail3.example.com> reportingconfig
Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]> mode
Centralized reporting: Local reporting only.
Do you want to enable centralized reporting? [N]> y
Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]>
```

데이터 보고용 스토리지 제한 구성(C-Series만)

```
mail.example.com> reportingconfig
Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]> mailsetup
SenderBase timeout used by the web interface: 5 seconds
Sender Reputation Multiplier: 3
The current level of reporting data recording is: unlimited
No custom second level domains are defined.
Legacy mailflow report: Disabled
Choose the operation you want to perform:
- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.
- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series before being
overwritten.
- LEGACY - Configure legacy mailflow report.
[]> storage
While in centralized mode the C-series will store reporting data for the M-series to collect.

If the M-series does not collect that data then eventually the C-series will begin to
overwrite the oldest data with new data.
A maximum of 24 hours of reporting data will be stored.
How many hours of reporting data should be stored before data loss?
[24]> 48
SenderBase timeout used by the web interface: 5 seconds
Sender Reputation Multiplier: 3
The current level of reporting data recording is: unlimited
No custom second level domains are defined.
Legacy mailflow report: Disabled
Choose the operation you want to perform:
- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.
- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series
before being overwritten.
- LEGACY - Configure legacy mailflow report.
[]>
```

Senderbase

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [sbstatus, 264 페이지](#)
- [senderbaseconfig, 264 페이지](#)

sbstatus

설명

SenderBase 쿼리의 상태를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> sbstatus
SenderBase host status
Status as of:      Tue Oct 21 10:55:04 2003
Host up/down:     up
```

어플라이언스에서 SenderBase Reputation Service에 연결할 수 없거나 서비스가 연결된 적이 없을 경우 다음 내용이 표시됩니다.

```
mail3.example.com> sbstatus
SenderBase host status
Host up/down:     Unknown (never contacted)
```

senderbaseconfig

설명

SenderBase 연결 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> senderbaseconfig
Share statistics with SenderBase Information Service: Enabled
Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
[]> setup
Do you want to share statistical data with the SenderBase Information Service (recommended)?
[Y]>
Share statistics with SenderBase Information Service: Enabled
Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
[]>
```

발신자 도메인 평판 필터링

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [sdrconfig, 265 페이지](#)
- [sdradvancedconfig, 266 페이지](#)
- [sdrstatus, 267 페이지](#)
- [sdrdiagnostics, 268 페이지](#)
- [sdrupdate, 268 페이지](#)

sdrconfig

- [설명, 265 페이지](#)
- [Usage\(사용\), 265 페이지](#)
- [예, 266 페이지](#)

설명

sdrconfig 명령은 Cisco Email Security 게이트웨이에서 SDR 필터링을 활성화하는 데 사용됩니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help sdrconfig` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

다음 예에서는 `sdrconfig` 명령을 사용하여 Cisco Email Security 게이트웨이에서 SDR 필터링을 활성화할 수 있습니다.

```
mail.example.com > sdrconfig

Would you like to enable sender domain reputation check? [N]> yes

SDR uses headers such as 'Envelope-From:', 'From:' and 'Reply-to' to determine the reputation
of the message.
In addition, it also uses the results of the email authentication mechanisms such as SPF,
DKIM, and DMARC
to decide the reputation.
The following additional attributes of the message can also be included in the Sender Domain
Reputation
check to improve the efficacy:

- Username part of the email address present in the 'Envelope-From:', 'From:' and 'Reply-To:'
headers.
- Display name in the 'From:' and 'Reply-To:' headers.

Do you want to include these additional attributes of the message for the Sender Domain
Reputation check? [N]> yes

Sender Domain Reputation (SDR) is a new feature in AsyncOS 12.0 that sends certain telemetry
data to Cisco.
If you choose to enable the 'Additional Attributes' function in SDR, that telemetry data
will include
the processing of personal data as described in the Cisco ESA Privacy Data Sheet
(https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html) and
the
Cisco Online Privacy Statement (https://www.cisco.com/c/en\_in/about/legal/privacy-full.html).

To enable the "Additional Attributes" feature in SDR, you must agree to the Cisco Content
Security Supplemental
End User License Agreement
(https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html).
By selecting Yes, you agree to be bound to the Cisco Content Security Supplemental End User
License Agreement
(https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html).

I accept the Cisco Content Security Supplemental End User License Agreement. [N]> yes
```

sdradvancedconfig

- 설명, 266 페이지
- Usage(사용), 267 페이지
- 예, 267 페이지

설명

`sdradvancedconfig` 명령은 Cisco Email Security 게이트웨이를 SDR 서비스에 연결할 때 고급 파라미터를 구성하는 데 사용됩니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help sdradvancedconfig` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

다음 예에서는 `sdradvancedconfig` 명령을 사용하여 Cisco Email Security 게이트웨이를 SDR 서비스에 연결할 때 고급 파라미터를 구성할 수 있습니다.

```
mail.example.com > sdradvancedconfig

Enter SDR query timeout in seconds [5]> 3

Enter the Domain Reputation service hostname [v2.beta.sds.cisco.com]>

Do you want to verify server certificate? [Y]>

Enter the default debug log level for RPC server: [Info]>

Enter the default debug log level for HTTP Client: [Info]>

Do you want exception list matches based on envelope-from domain only? [Y]>
```

sdrstatus

- [설명, 267 페이지](#)
- [Usage\(사용\), 267 페이지](#)
- [예, 267 페이지](#)

설명

`sdrstatus` 명령은 SDR 구성 요소의 현재 버전을 표시하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 `sdrstatus` 명령을 사용하여 SDR 구성 요소의 현재 버전을 볼 수 있습니다.

```
mail.example.com> sdrstatus
```

Component	Version	Last Updated
SDR Client	1.0	2 Jul 2018 04:22 (GMT +00:00)

sdrupdate

- [설명, 268 페이지](#)
- [Usage\(사용\), 268 페이지](#)
- [예, 268 페이지](#)

설명

sdrupdate 명령은 SDR 구성 요소를 수동으로 업데이트하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 sdrupdate 명령을 사용하여 SDR 구성 요소를 수동으로 업데이트할 수 있습니다.

```
mail.example.com > sdrupdate
```

```
Requesting update of Sender Domain Reputation component.
```

sdrdiagnostics

- [설명, 268 페이지](#)
- [Usage\(사용\), 268 페이지](#)
- [예, 269 페이지](#)

설명

sdrdiagnostics 명령은 게이트웨이가 SDR 서비스에 연결되어 있는지 확인하는 데 사용됩니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 `sdrdiagnostics` 명령을 사용하여 Cisco Email Security 게이트웨이가 SDR 서비스에 연결되어 있는지 확인할 수 있습니다.

```
mail.example.com > sdrdiagnostics

1. Show status of the domain reputation service
[1]> 1
Connection Status: Connected
```

Smart Software Licensing

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [license_smart, 269 페이지](#)

license_smart

- [설명, 269 페이지](#)
- [Usage\(사용\), 269 페이지](#)
- [예: Smart Agent 서비스용 포트 구성, 270 페이지](#)
- [예: Smart Licensing 활성화, 270 페이지](#)
- [예: Smart Software Manager에 어플라이언스 등록, 270 페이지](#)
- [예: Smart Licensing의 상태, 270 페이지](#)
- [예: Smart Licensing의 상태 요약, 271 페이지](#)
- [예: Smart Transport URL 설정, 271 페이지](#)
- [예: 라이선스 요청, 272 페이지](#)
- [예: 라이선스 해제, 272 페이지](#)

설명

Smart Software Licensing 기능을 구성합니다.

Usage(사용)

커밋: 이 명령은 '커밋'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드에서만 사용할 수 있습니다. 이 명령은 클러스터 및 그룹 모드를 지원하지 않습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help license_smart` 명령을 입력하여 온라인 도움말을 참고하십시오.

예: Smart Agent 서비스용 포트 구성

```
mail.example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

예: Smart Licensing 활성화

```
mail.example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
[]> enable
After enabling Smart Licensing on your appliance, follow below steps to activate the feature
keys (licenses):
a) Register the product with Smart Software Manager using license_smart > register command
in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.
Note: If you are using a virtual appliance, and have not enabled any of the features in the
classic licensing mode; you will not be able to activate the licenses, after you switch
to the smart licensing mode. You need to first register your appliance, and then you can
activate the licenses (features) in the smart licensing mode.
Commit your changes to enable the Smart Licensing mode on your appliance. All the features
enabled in the Classic Licensing mode will be available in the Evaluation period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
[Y/N] []> y
> commit
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

예: Smart Software Manager에 어플라이언스 등록

```
mail.example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
[]> register
Reregister this product instance if it is already registered [N]> n
Enter token to register the product:
[]> ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR
8WlpCQ1lMbGVMQWRxOXhuenN4OWZDdktFckJLQzF5V3VlBzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
registration.
```

예: Smart Licensing의 상태

```
mail.example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
```

```

- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
[ ]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
Virtual Account: Not Available
Smart Account: Not Available
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: mail.example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)

```

예: Smart Licensing의 상태 요약

```

mail.example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
[ ]> summary
FeatureName                               LicenseAuthorizationStatus
Mail Handling                               Eval
Email Security Appliance Bounce Verification Eval
Email Security Appliance Outbreak Filters  Eval

```

예: Smart Transport URL 설정

```

mail.example.com> license_smart
Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
[ ]> url
1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
   satellite.
Choose from the following menu options:
[1]> direct
You must enter a value from 1 to 2.
1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
   satellite.
Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command.
Transport settings will be updated after commit.

```

예: 라이선스 요청



참고 가상 어플라이언스의 사용자가 라이선스를 요청하거나 릴리스하려면 해당 어플라이언스를 등록해야 합니다.

```
mail.example.com> license_smart
Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
[> requestsmart_license
Feature Name                                     License Authorization Status
1. Email Security Appliance Sophos Anti-Malware   Not Requested
2. Email Security Appliance PXE Encryption        Not requested

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[> 1
Activation is in progress for following features:
Email Security Appliance Sophos Anti-Malware
Use license_smart > summary command to check status of licenses.
```

예: 라이선스 해제

```
mail.example.com> license_smart
Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
[> releasesmart_license
Feature Name                                     License Authorization Status
1. Email Security Appliance Anti-Spam License     Eval
2. Email Security Appliance Outbreak Filters      Eval
3. Email Security Appliance Graymail Safe-unsubscribe Eval
4. Email Security Appliance Cloudmark Anti-Spam   Eval
5. Mail Handling                                  Eval
6. Email Security Appliance Sophos Anti-Malware   Eval
7. Email Security Appliance PXE Encryption        Eval
8. Email Security Appliance Advanced Malware Protection Eval

Enter the appropriate license number(s) for deactivation.
Separate multiple license with comma or enter range:
[>
```

show_license

- [설명, 273 페이지](#)
- [예: Smart Licensing의 상태, 273 페이지](#)

- 예: [Smart Licensing의 상태 요약, 273 페이지](#)

설명

Smart Licensing 상태 및 상태 요약을 표시합니다.

예: Smart Licensing의 상태

```
mail.example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
Virtual Account: Not Available
Smart Account: Not Available
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: mail.example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

예: Smart Licensing의 상태 요약

```
mail.example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary



| FeatureName                                  | LicenseAuthorizationStatus |
|----------------------------------------------|----------------------------|
| Mail Handling                                | Eval                       |
| Email Security Appliance Bounce Verification | Eval                       |
| Email Security Appliance Outbreak Filters    | Eval                       |


```

SMTP 서비스 컨피그레이션

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [callaheadconfig, 273 페이지](#)
- [listenerconfig, 275 페이지](#)
- [localeconfig, 305 페이지](#)
- [smtpauthconfig, 306 페이지](#)

callaheadconfig

설명

SMTP Call-Ahead 프로필을 추가, 수정, 제거합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 전달 호스트에 대해 새 SMTP call-ahead 프로필을 생성할 수 있습니다.

```
> callaheadconfig
No SMTP Call-Ahead profiles are configured on the system.
Choose the operation you want to perform:
- NEW - Create a new profile.
[ ]> new
Select the type of profile you want to create:
1. Delivery Host
2. Static Call-Ahead Servers
[1]> 1
Please enter a name for the profile:
[ ]> delhost01
Advanced Settings:
  MAIL FROM Address: <>
  Interface: Auto
  Timeout Value: 30
  Validation Failure Action: ACCEPT
  Temporary Failure Action: REJECT with same code
  Maximum number of connections: 5
  Maximum number of validation queries: 1000
  Cache size: 10000
  Cache TTL: 900
Do you want to change advanced settings? [N]> n
Currently configured SMTP Call-Ahead profiles:
1. delhost01 (Delivery Host)
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[ ]>
```

다음 예에서는 call-ahead 서버에 대해 새 SMTP call-ahead 프로필을 생성할 수 있습니다.

```
> callaheadconfig
Currently configured SMTP Call-Ahead profiles:
1. delhost01 (Delivery Host)
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[ ]> new
Select the type of profile you want to create:
1. Delivery Host
2. Static Call-Ahead Servers
```

```
[1]> 2
Please enter a name for the profile:
[]> Static
Enter one or more Call-Ahead servers hostname separated by commas.
[]> 192.168.1.2
Advanced Settings:
  MAIL FROM Address: <>
  Interface: Auto
  Timeout Value: 30
  Validation Failure Action: ACCEPT
  Temporary Failure Action: REJECT with same code
  Maximum number of connections: 5
  Maximum number of validation queries: 1000
  Cache size: 10000
  Cache TTL: 900
Do you want to change advanced settings? [N]> n
Currently configured SMTP Call-Ahead profiles:
1. Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]> print
Select the profile you want to print:
1. Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)
[1]>
```

listenerconfig

설명

listenerconfig 명령을 사용하여 리스너를 생성, 수정 및 삭제할 수 있습니다. AsyncOS에서는 메시지가 수락되고 수신자 호스트(네트워크 내부 또는 인터넷으로 연결된 외부 수신자)에 릴레이되기 위해 충족할 기준을 지정해야 합니다.

이러한 자격 기준이 리스너에 정의됩니다. 종합적으로 리스너는 메일 플로우 정책을 정의하고 시행합니다. Listener는 어플라이언스에서 이메일을 주입하는 시스템과 통신하는 방법도 정의합니다.

표 13: listenerconfig 명령

이름	향후 참조를 위해 리스너에 제공하는 고유한 별칭. 리스너에 대해 정의하는 이름은 대/소문자를 구분합니다. AsyncOS에서는 2개의 동일한 리스너 이름을 생성할 수 없습니다.
IP 인터페이스	리스너는 IP 인터페이스에 지정됩니다. 리스너를 생성하여 지정하려면 먼저 systemstartup 명령 또는 interfaceconfig 명령을 사용하여 모든 IP 인터페이스를 성해야 합니다.
메일 프로토콜	메일 프로토콜은 이메일 수신에 사용됩니다. ESMTP 또는 QMQP입니다.

IP 포트	리스너와의 연결에 사용되는 IP 포트입니다. 기본적으로 SMTP는 포트 25를, QMQP는 포트 628을 사용합니다.
리스너 유형: 공용 전용 블랙홀	공용 및 전용 리스너가 대부분의 컨피그레이션에 사용됩니다. 일반적으로 전용 리스너는 전용(내부) 네트워크에 사용하며, 공용 리스너는 인터넷에서 이메일을 수신하기 위한 기본 특성을 포함합니다. “블랙홀(Blackhole)” 리스너는 테스트 또는 트러블슈팅 용도로 사용할 수 있습니다. 블랙홀 리스너를 생성할 경우 메시지를 삭제하기 전에 디스크에 기록할지 여부를 선택합니다. 자세한 내용은 <i>AsyncOS for Cisco Email Security Appliance</i> 사용 설명서의 "테스트 및 트러블슈팅" 장을 참조하십시오.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형 - 일반 listenerconfig

listenerconfig 명령의 배치 형식을 사용하여 특정 인터페이스에서 리스너를 추가하고 삭제할 수 있습니다. listenerconfig 명령의 배치 형식으로 리스너의 HAT 및 RAT를 구성할 수도 있습니다.

- 새 리스너 추가:

```
listenerconfig new <name> <public|private|blackhole|blackholequeueing>
<interface_name> <smtp|qmqp>
```

- 리스너 삭제:

```
listenerconfig delete <name>
```

배치 형식 - HAT

다음 예에서는 다양한 HAT 관련 작업에 listenerconfig의 배치 형식을 사용하는 것을 보여줍니다. 인수에 대한 자세한 내용은 아래의 표 - listenerconfig 인수 값 -HAT를 참고하십시오.

- HAT에 발신자 그룹 추가

```
listenerconfig edit <name> hostaccess new sendergroup <name> <host_list> <behavior>
[options [--comments]
```

- HAT에 새 정책 추가


```
listenerconfig edit <name> hostaccess new policy <name> <behavior> [options]
```

- 발신자 그룹에 새 호스트 목록 추가

```
listenerconfig edit <name> hostaccess edit sendergroup <name> new <host_list>
```

- 발신자 그룹에서 호스트 삭제

```
listenerconfig edit <name> hostaccess edit sendergroup <name> delete <host>
```

- 발신자 그룹 목록에서 호스트의 순서 이동

```
listenerconfig edit <name> hostaccess edit sendergroup <name> move <host>
<host-to-insert-before>
```

- 발신자 그룹 정책 수정

```
listenerconfig edit <name> hostaccess edit sendergroup <name> policy <behavior> [options]
```

- 발신자 그룹 목록 인쇄

```
listenerconfig edit <name> hostaccess edit sendergroup <name> print
```

- 발신자 그룹 이름 변경

```
listenerconfig edit <name> hostaccess edit sendergroup <name> rename <name>
```

- HAT 정책 수정

```
listenerconfig edit <name> hostaccess edit policy <name> <behavior> [options]
```

- HAT에서 발신자 그룹 삭제

```
listenerconfig edit <name> hostaccess delete sendergroup <name>
```

- 정책 삭제

```
listenerconfig edit <name> hostaccess delete policy <name>
```

- HAT에서 발신자 그룹의 위치 이동

```
listenerconfig edit <name> hostaccess move <group> <group-to-insert-before>
```

- HAT 기본 옵션 변경

```
listenerconfig edit <name> hostaccess default [options]
```

- 호스트 액세스 테이블 인쇄

```
listenerconfig edit <name> hostaccess print
```

- HAT의 로컬 복사본 가져오기

```
listenerconfig edit <name> hostaccess import <filename>
```

- 어플라이언스에서 HAT 복사본 내보내기

```
listenerconfig edit <name> hostaccess export <filename>
```

- HAT에서 모든 사용자 정의 발신자 그룹 및 정책 삭제

```
listenerconfig edit <name> hostaccess clear
```

- 특정 발신자 그룹에 대한 발신자의 발신지 국가 추가.

```
listenerconfig edit incoming hostaccess edit sendergroup WHITELIST  
country add India Nepal Cyprus
```

- 특정 발신자 그룹에 대한 발신자의 발신지 국가 삭제.

```
listenerconfig edit incoming hostaccess edit sendergroup WHITELIST  
country delete Cyprus
```

- 특정 발신자 그룹에 대한 발신자의 발신지 국가 인쇄.

```
listenerconfig edit incoming hostaccess edit sendergroup WHITELIST  
country print
```

표 14: listenerconfig 인수 값 -HAT

인수	설명
<behavior>	“Accept”, “Relay”, “Reject”, “TCP Refuse” 또는 “Continue”입니다. 발신자 그룹과 함께 사용할 동작을 선택할 때 “Policy: FOO” 형식의 추가 동작을 사용할 수 있습니다(“FOO”는 정책의 이름).
<filename>	호스트 액세스 테이블을 가져오고 내보낼 때 사용할 파일 이름입니다.
<group>	발신자 그룹의 <name>입니다.
<host>	<host_list>의 단일 엔티티입니다.

인수	설명
<host_list>	<p>추가할 호스트를 입력합니다. 다음 형식으로 호스트를 입력할 수 있습니다.</p> <p>CIDR 주소 (10.1.1.0/24)</p> <p>IP 주소 범위(10.1.1.10-20)</p> <p>IP 서브넷(10.2.3)</p> <p>호스트 이름(crm.example.com)</p> <p>부분적 호스트 이름(.example.com)</p> <p>발신자 기본 평판 점수 범위(7.5:10.0)</p> <p>Senderbase 네트워크 소유자 IDS(SBO: 12345)</p> <p>원격 블랙리스트 쿼리(dnslist [query.blacklist.example])</p> <p>참고 여러 호스트는 쉼표로 구분합니다.</p>
<name>	발신자 그룹 또는 정책의 이름입니다. HAT 레이블은 글자나 밑줄로 시작하고 그 뒤에 임의 개수의 문자, 숫자, 밑줄 또는 하이픈으로 구성됩니다.
[옵션]	
--max_size	최대 메시지 크기입니다. 킬로바이트는 k, 메가바이트는 M을 뒤에 붙이며 바이트는 어떤 문자도 붙이지 않습니다.
--max_conn	단일 호스트에서 허용되는 최대 연결 수입니다.
--max_msgs	연결당 최대 메시지 수입니다.
--max_rcpt	메시지당 최대 수신자 수입니다.
--override	SMTP 배너에서 호스트 이름을 재지정합니다. “No” 또는 SMTP 배너 문자열입니다.
--cust_acc	사용자 지정 SMTP 수락 응답을 지정합니다. “No” 또는 SMTP 수락 응답 문자열입니다.
--acc_code	사용자 지정 SMTP 수락 응답 코드입니다. 기본값은 220입니다.
--cust_rej	사용자 지정 SMTP 거부 응답을 지정합니다. “No” 또는 SMTP 거부 응답 문자열입니다.
--rej_code	사용자 지정 SMTP 거부 응답 코드입니다. 기본값은 554입니다.
--rate_lim	호스트당 속도 제한을 활성화합니다. “No”, “default” 또는 호스트별 시간당 최대 수신자 수입니다.
--cust_lim	사용자 지정 SMTP 제한 초과 응답 메시지를 지정합니다. “No” 또는 SMTP 거부 응답 문자열입니다. 기본값은 “No”입니다.

인수	설명
--lim_code	사용자 지정 SMTP 제한 초과 응답 코드입니다. 기본값은 452입니다.
--use_sb	기본적으로 흐름 제어에 SenderBase를 사용합니다. “Yes”, “No” 또는 “default”입니다.
--as_scan	안티스팸 검사를 활성화합니다. “Yes”, “No” 또는 “Default”입니다.
--av_scan	안티바이러스 검사를 활성화합니다. “Yes”, “No” 또는 “Default”입니다.
--dhap	디렉터리 수집 공격 방지입니다. “No”, “default” 또는 원격 호스트의 시간당 잘못된 수신자 최대 수입니다.
--tls	지원되지 않습니다. 메뉴 시스템을 사용하여 TLS를 구성합니다.
--sig_bits	IT 주소에서 유효 비트로 처리할 비트 수입니다. 0~32, “No” 또는 “default”입니다.
--dkim_signing	DKIM 서명을 활성화합니다. “Yes”, “No” 또는 “Default”입니다.
--dkim_verification	DKIM 확인을 활성화합니다. “Yes”, “No” 또는 “Default”입니다.
--dkim_verification_profile <name>	DKIM 확인 프로필의 이름입니다. 이 옵션은 --dkim_verification의 값이 “Yes”로 설정된 경우에만 사용 가능합니다.
--spf	SPF 확인을 활성화합니다. “Yes”, “No” 또는 “Default”입니다.
--spf_conf_level	SPF 적합성 레벨입니다. 오로지 “--spf Yes”와 함께 사용합니다. “spf_only”, “sidf_compatible” 또는 “sidf_strict”입니다.
--spf_downgrade_pra	SPF PRA 확인 결과를 다운그레이드합니다. 오로지 “--spf Yes” 및 “--spf_conf_level sidf_compatible”과 함께 사용합니다. “Yes” 또는 “No”입니다.
--spf_helo_test	SPF HELO 테스트입니다. “--spf Yes” 및 “--spf_conf_level sidf_compatible” 또는 “--spf_conf_level spf_only”와 함께 사용합니다. “Yes” 또는 “No”입니다.
--dmarc_verification	DMARC 확인을 활성화합니다. “Yes”, “No” 또는 “Default”입니다.
--dmarc_verification_profile <name>	DMARC 확인 프로필의 이름입니다. 이 옵션은 --dmarc_verification의 값이 “Yes”로 설정된 경우에만 사용 가능합니다.
--dmarc_agg_reports	DMARC 집계 보고서를 활성화합니다. “Yes”, “No” 또는 “Default”입니다. 이 옵션은 --dmarc_verification의 값이 “Yes”로 설정된 경우에만 사용 가능합니다.

배치 형식 - RAT

다음 예에서는 다양한 RAT 관련 작업에 listenerconfig의 배치 형식을 사용하는 것을 보여줍니다. 인수에 대한 자세한 내용은 아래의 표 - *listenerconfig* 인수 값 -RAT를 참고하십시오.

- RAT에 새 수신자 추가

```
listenerconfig edit <name> rcptaccess new <rat_addr> [options]
```

- RAT의 수신자 수정

```
listenerconfig edit <name> rcptaccess edit <rat_addr> [options]
```

- RAT에서 수신자 삭제

```
listenerconfig edit <name> rcptaccess delete <rat_addr>
```

- RAT의 복사본 인쇄

```
listenerconfig edit <name> rcptaccess print
```

- 어플라이언스에 로컬 RAT 가져오기

```
listenerconfig edit <name> rcptaccess import <filename>
```

- RAT 내보내기

```
listenerconfig edit <name> rcptaccess export <filename>
```

- 기본 액세스 지우기

```
listenerconfig edit <name> rcptaccess clear <default_access>
```

표 15: listenerconfig 인수 값 - RAT

인수	설명
<rat_addr>	추가할 호스트를 입력합니다. 다음 형식으로 호스트를 입력할 수 있습니다. CIDR 주소 (10.1.1.0/24) 호스트 이름(crm.example.com) 부분적 호스트 이름(.example.com) 사용자 이름(postmaster@) 전체 이메일 주소(joe@example.com, joe@[1.2.3.4]) 참고 여러 호스트는 쉼표로 구분합니다.
<options>	
--action	주소에 적용할 작업입니다. "Accept" 또는 "Reject"입니다. 기본값은 "Accept"입니다.
--cust_resp	사용자 지정 SMTP 응답을 지정합니다. "No" 또는 SMTP 수락 응답 문자열입니다.
--resp_code	사용자 지정 SMTP 응답 코드입니다. 기본값은 "Accept"라면 250, "Reject"라면 550입니다.
--bypass_rc	수신 제어를 바이패스합니다. 기본값은 "No"입니다.
--bypass_la	LDAP Accept 쿼리를 바이패스합니다. "Yes" 또는 "No"입니다.
--bypass_ca	SMTP Call-Ahead를 우회합니다. 기본값은 "No"입니다.

예 - 리스너 추가

다음 예에서는 listenerconfig 명령을 사용하여 Enterprise Gateway 컨피그레이션에 필요한 B 리스너에 사용 가능한 OutboundMail이라는 새 전용 리스너를 생성합니다. GUI의 System Setup Wizard(시스템 설정 마법사) CLI **systemsetup** 명령에서 이 전용 리스너를 추가할 수도 있습니다.

전용 리스너 유형을 선택하고 이름을 OutboundMail로 지정합니다. 포트 25에서 SMTP 프로토콜을 사용하여 PrivateNet IP 인터페이스에서 실행하도록 지정됩니다. 그런 다음 이 리스너에 대한 호스트 액세스 정책의 기본값이 수락됩니다.

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
```

```

[1]> new
Please select the type of listener you want to create.
1. Private
2. Public
3. Blackhole
[2]> 1
Please create a name for this listener (Ex: "OutboundMail"):
[1]> OutboundMail
Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 2
Choose a protocol.
1. SMTP
2. QMQP
[1]> 1
Please enter the TCP port for this listener.
[25]> 25
Please specify the systems allowed to relay email through the IronPort C60.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[1]> .example.com
Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum
number of recipients per hour you are
willing to receive from a remote domain.)      [N]> n
Default Policy Parameters
=====
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 600
Maximum Number Of Messages Per Connection: 10,000
Maximum Number Of Recipients Per Message: 100,000
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: No
Spam Detection Enabled: No
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Would you like to change the default host access policy? [N]> n
Listener OutboundMail created.
Defaults have been set for a Private listener.
Use the listenerconfig->EDIT command to customize the listener.
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[1]>

```

예 - 발신자 그룹에 발신자의 발신지 국가 추가

다음 예에서는 `listenerconfig` 명령을 사용하여 특정 발신자 그룹에 대한 발신자의 발신지 국가를 추가하기 위해 리스너를 수정합니다.

```
mail3.example.com> listenerconfig
```

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[> edit

Enter the name or number of the listener you wish to edit.

[> 1

Name: InboundMailhostacce

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: off

Choose the operation you want to perform:

- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.


```
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.

[]> hostaccess

Default Policy Parameters

=====

Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
```

```

- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.

[> edit
1. Edit Sender Group
2. Edit Policy

[1]>1
Currently configured HAT sender groups:
1. WHITELIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLACKLIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. MyList
6. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.

[> 1
Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- COUNTRY - Add and delete countries.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.

[> country
Choose the operation you want to perform:
- ADD - Add countries

[>ADD
1. Afghanistan [af]
2. Aland Islands [ax]
3. Albania [al]

```

```

4. Algeria [dz]
5. American Samoa [as]
6. Andorra [ad]
7. Angola [ao]
8. Anguilla [ai]
9. ...

Enter the indices separated by commas or specify the range.

[>]1,4,8

Choose the operation you want to perform:

- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- COUNTRY - Add and delete countries.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.

[>] country

Choose the operation you want to perform:

- ADD - Add countries
- DELETE - Delete countries
- PRINT - Print countries

[>] print

Afghanistan [af]

Algeria [dz]

Anguilla [ai]

```

예 - 내보내기 및 가져오기를 통해 리스너에 대한 HAT(Host Access Table) 사용자 정의

`listenerconfig` 명령의 여러 하위 명령을 사용하면 CLI에서 데이터를 단편적으로 입력할 필요 없이 데이터 가져오기 및 내보내기를 통해 대규모 컨피그레이션 변경 사항을 적용할 수 있습니다.

이 단계에서는 CLI를 사용하여 파일 내보내고 수정하고 가져오는 방법으로 리스너의 HAT(Host Access Table)를 수정합니다. HAT CLI 편집기나 GUI를 사용하여 리스너에 대한 HAT를 사용자 정의할 수도 있습니다. 자세한 내용은 *AsyncOS for Cisco Email Security Appliance* 사용자 가이드의 "메일 수신에 위한 게이트웨이 구성" 및 "메일 흐름 모니터 사용" 장을 참고하십시오.

내보내기 및 가져오기를 통해 정의한 리스너에 대한 HAT를 사용자 정의하려면

프로시저

단계 1 기본 HAT를 파일에 내보내려면 listenerconfig의 hostaccess -> export 하위 명령을 사용합니다.

다음 예에서는 공용 리스너 InboundMail의 HAT를 인쇄한 다음 inbound.HAT.txt라는 파일에 내보냅니다.

예제:

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[> edit
Enter the name or number of the listener you wish to edit.
[> 1
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[> hostaccess
Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
```

```

Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[ ]> print
$BLOCKED
  REJECT {}
$TRUSTED
  ACCEPT {
    tls = "off"
    dhap_limit = 0
    max_rcpts_per_hour = -1
    virus_check = "on"
    max_msgs_per_session = 5000
    spam_check = "off"
    use_sb = "off"
    max_message_size = 104857600
    max_rcpts_per_msg = 5000
    max_concurrency = 600
  }
$ACCEPTED
  ACCEPT {}
$THROTTLED
  ACCEPT {
    tls = "off"
    dhap_limit = 0
    max_rcpts_per_hour = 1
    virus_check = "on"
    max_msgs_per_session = 10
    spam_check = "on"
    use_sb = "on"
    max_message_size = 1048576
    max_rcpts_per_msg = 25
    max_concurrency = 10
  }
WHITELIST:
  $TRUSTED (My trusted senders have no anti-spam or rate limiting)
BLACKLIST:
  $BLOCKED (Spammers are rejected)
SUSPECTLIST:
  $THROTTLED (Suspicious senders are throttled)
UNKNOWNLIST:
  $ACCEPTED (Reviewed but undecided, continue normal acceptance)
ALL
  $ACCEPTED (Everyone else)
Default Policy Parameters
=====

```

```

Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[> export
Enter a name for the exported file:
[> inbound.HAT.txt
File written on machine "mail3.example.com".

```

예제:

단계 2 CLI(명령줄 인터페이스) 외부에서 inbound.HAT.txt 파일을 가져옵니다.

단계 3 텍스트 편집기로 파일에 새 HAT 항목을 생성합니다.

이 예에서는 HAT에서 ALL 항목의 위에 다음 항목을 추가합니다.

spamdomain.com	REJECT
.spamdomain.com	REJECT
251.192.1.	TCPREFUSE
169.254.10.10	RELAY

- 처음 2개 항목은 도메인 spamdomain.com 및 해당 하위 도메인에 속한 원격 호스트로부터의 모든 연결을 거부합니다.
- 세 번째 라인에서는 IP 주소가 251.192.1.x인 모든 호스트의 연결을 거부합니다.
- 네 번째 라인에서는 IP 주소가 169.254.10.10인 원격 호스트에서 Email Security Appliance를 모든 인터넷 아웃바운드 이메일의 SMTP 릴레이로 사용하는 것을 허용합니다.

참고 HAT에서 규칙이 나타나는 순서가 중요합니다. 리스너에 연결하려고 시도하는 각 호스트에 대해 위에서 아래로 HAT를 읽습니다. 어떤 규칙이 연결 호스트와 매치할 경우 그 연결에 대한 작업이 즉시 수행됩니다. HAT에서 모든 사용자 정의 항목이 ALL 호스트 정의의 위에 있어야 합니다. HAT CLI 편집기나 GUI를 사용하여 리스너에 대한 HAT를 사용자 정의할 수도 있습니다. 자세한 내용은 *AsyncOS for Cisco Email Security Appliance* 사용자 가이드의 "메일 수신을 위한 게이트웨이 구성" 및 "메일 흐름 모니터 사용" 장을 참고하십시오.

단계 4 파일을 저장한 다음, 가져올 수 있도록 인터페이스의 configuration 디렉터리에 둡니다. 자세한 내용은 부록 B, “어플라이언스 액세스”를 참조하십시오.

단계 5 수정된 HAT 파일을 가져오려면 listenerconfig의 hostaccess -> import 하위 명령을 사용합니다.

다음 예에서는 수정된 파일 inbound.HAT.txt를 InboundMail 리스너의 HAT에 가져옵니다. print 하위 명령을 사용하여 새 항목을 인쇄합니다.

예제:

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
```

예 - 내보내기 및 가져오기를 통해 리스너에 대한 HAT(Host Access Table) 사용자 정의

```

- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[> import
Enter the name of the file to import:
[> inbound.HAT.txt
9 entries imported successfully.
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[> print
$ACCEPTED
  ACCEPT
$THROTTLED
  ACCEPT {
    spam_check = "on"
    max_msgs_per_session = 10
    max_concurrency = 10
    max_rcpts_per_msg = 25
    max_rcpts_per_hour = 1
    dhap_limit = 0
    virus_check = "on"
    max_message_size = 1048576
    use_sb = "on"
    tls = "off"
  }
$TRUSTED
  ACCEPT {
    spam_check = "off"
    max_msgs_per_session = 5000
    max_concurrency = 600
    max_rcpts_per_msg = 5000
    max_rcpts_per_hour = -1
    dhap_limit = 0
    virus_check = "on"
    max_message_size = 104857600
    use_sb = "off"
  }

```



```

        tls = "off"
    }
$BLOCKED
  REJECT
WHITELIST:
  $TRUSTED (My trusted senders have no anti-spam scanning or rate limiting)
BLACKLIST:
  $BLOCKED (Spammers are rejected)
SUSPECTLIST:
  $THROTTLED (Suspicious senders are throttled)
UNKNOWNLIST:
  $ACCEPTED (Reviewed but undecided, continue normal acceptance)
spamdomain.com
  REJECT (reject the domain "spamdomain.com")
.spamdomain.com
  REJECT (reject all subdomains of ".spamdomain.com")
251.192.1.
  TCPREFUSE (TCPREFUSE the IP addresses in "251.192.1")
169.254.10.10
  RELAY (RELAY the address 169.254.10.10)
ALL
  $ACCEPTED (Everyone else)
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]>

```

가져오기한 다음 **commit** 명령을 실행해야 컨피그레이션 변경이 적용됩니다.

예 - 공개 키 수집 및 S/MIME 해독/확인 활성화

이번 예에서는 다음 방법을 보여줍니다.

- 수신 S/MIME 서명 메시지에서 (수집) 공개 키 검색
- S/MIME 해독 및 확인 활성화

```
mail.example.com> listenerconfig
```

```

Currently configured listeners:
1. MyListener (on Management, 172.29.181.70) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[ ]> edit
Enter the name or number of the listener you wish to edit.
[ ]> 1
Name: MyListener
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 50 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[ ]> hostaccess

Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: No
S/MIME Decryption/Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.

```

```

There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[ ]> default
Enter the default maximum message size. Add a trailing k for kilobytes, M for megabytes,
or no letter for b
[10M]>
Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>
Enter the maximum number of messages per connection.
[10]>
Enter the maximum number of recipients per message.
[50]>
Do you want to override the hostname in the SMTP banner? [N]>
Would you like to specify a custom SMTP acceptance response? [N]>
Would you like to specify a custom SMTP rejection response? [N]>
Do you want to enable rate limiting per host? [N]>
Do you want to enable rate limiting per envelope sender? [N]>
Do you want to enable Directory Harvest Attack Prevention per host? [Y]>
Enter the maximum number of invalid recipients per hour from a remote host.
[25]>
Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>
Would you like to specify a custom SMTP DHAP response? [Y]>
Enter the SMTP code to use in the response. 550 is the standard code.
[550]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
custom_response
Would you like to use SenderBase for flow control by default? [Y]>
Would you like to enable anti-spam scanning? [Y]>
Would you like to enable anti-virus scanning? [Y]>
Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>
Would you like to enable DKIM/DomainKeys signing? [N]>
Would you like to enable DKIM verification? [N]>
Would you like to enable S/MIME Public Key Harvesting? [N]> y

Would you like to harvest certificate on verification failure? [N]>

Would you like to harvest updated certificate? [Y]>

Would you like to enable S/MIME gateway decryption/verification? [N]> y

Select the appropriate operation for the S/MIME signature processing:
1. Preserve
2. Remove
[1]>
Would you like to change SPF/SIDF settings? [N]>
Would you like to enable DMARC verification? [N]>

```

Example - 고급 HAT 매개변수

```

Would you like to enable envelope sender verification? [N]>
Would you like to enable use of the domain exception table? [N]>
Do you wish to accept untagged bounces? [N]>
Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: Yes
S/MIME Decryption/Verification Enabled: Yes
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]>

```

Example - 고급 HAT 매개변수

다음 표에서는 고급 HAT 매개변수의 구문을 정의합니다. 아래의 숫자 값에서 후행 **k**를 추가하여 킬로바이트를 나타내거나 후행 **M**을 추가하여 메가바이트를 나타낼 수 있습니다. 문자가 없는 값은 바이트로 간주됩니다. 다음 표에 별표로 표시된 매개변수는 예 나와 있는 변수 구문을 지원합니다.

표 16: 고급 HAT 매개변수 구문

매개변수	구문	값	값 예
연결당 최대 메시지 수	max_msgs_per_session	번호	1000
Maximum recipients per message(메시지당 최대 수신자 수)	max_rcpts_per_msg	번호	10000 1k

매개변수	구문	값	값 예
최대 메시지 크기	max_message_size	번호	1048576 20M
이 리스너에 대해 허용되는 최대 동시 연결 수	max_concurrency	번호	1000
SMTP 배너 코드	smtp_banner_code	번호	220
SMTP 배너 텍스트 (*)	smtp_banner_text	문자열	Accepted
SMTP 거부 배너 코드	smtp_banner_code	번호	550
MTP 거부 배너 텍스트 (*)	smtp_banner_text	문자열	Rejected
SMTP 배너 호스트 이름 덮어쓰기	use_override_hostname	on off default	default
	override_hostname	문자열	newhostname
Use TLS(TLS 사용)	tls	on off required	on
Use anti-spam scanning(안티스팸 검사 사용)	spam_check	on off	off
Use Sophos virus scanning(Sophos 바이러스 검사 사용)	virus_check	on off	off
시간당 최대 수신자 수	max_rcpts_per_hour	번호	5k
시간당 최대 수신자 수 오류 코드	max_rcpts_per_hour_code	번호	452
시간당 최대 수신자 수 텍스트 (*)	max_rcpts_per_hour_text	문자열	Too manyrecipients
SenderBase 사용	use_sb	on off	on
SenderBase Reputation 점수 정의	sbrs[value1 :value2]	-10.0- 10.0	sbrs[-10:-7.5]
DHAP(Directory Harvest Attack Prevention): 시간당 최대 잘못된 수신자 수	dhap_limit	번호	150

listenerconfig에 bypass_ca 인수 추가

다음 예에서는 listenerconfig에 bypass_ca 인수를 추가하는 방법을 보여 줍니다.

```
esa.example.com (SERVICE)> help listenerconfig.
```

```
rcptaccess_options are the following:
  new <rat_addr> [options]
  edit <rat_addr> [options]
  delete <rat_addr>
  print
  import <filename>
  export <filename>
  clear <default_access>

  default_access - Default access for empty RAT.  Either "ACCEPT"
                  or "REJECT".
  rat_addr - Hostnames such as "example.com" and "[1.2.3.4]" are
             allowed. Partial hostnames such as ".example.com"
             are allowed. Usernames such as "postmaster@" are
             allowed. Full email addresses such as
             "joe@example.com" or "joe@[1.2.3.4]" are allowed.
             Separate multiple entries with commas.
  options - Various options to modify a host access policy:
    --action      Action to apply to address(es).  Either
                  "Accept" or "Reject".  Default is "Accept".
    --cust_resp   Specify a custom SMTP response.  "No" or SMTP
                  acceptance response string.
    --resp_code   Custom SMTP response code.  Default is 250 for
                  "Accept" actions, 550 for "Reject".
    --bypass_rc   Bypass receiving control.  Default is "No".
    --bypass_la   Bypass LDAP Accept queries for this Recipient.  Default is "No".
    --bypass_ca   Bypass SMTP Call-Ahead.  Default is "No".
```

예 - SPF 및 SIDF 구성

리스너의 HAT에 대한 기본 설정을 구성할 때 리스너의 SPF/SIDF 적합성 레벨 및 SPF/SIDF 확인 결과에 따라 어플라이언스에서 수행하는 SMTP 작업(ACCEPT 또는 REJECT)을 선택할 수 있습니다. 또한 어플라이언스가 메시지 거부 시 전송하는 SMTP 응답을 정의할 수 있습니다.

적합성 레벨에 따라 어플라이언스는 HELO ID, MAIL FROM ID 또는 PRA ID에 대한 검사를 수행합니다. 각 ID 검사에 대한 다음 SPF/SIDF 확인 결과에 따라 어플라이언스가 세션을 계속 진행할지 (ACCEPT) 또는 세션을 끝낼지(REJECT)를 지정할 수 있습니다.

- **None.** 정보가 부족해 확인을 수행할 수 없습니다.
- **Neutral.** 클라이언트가 특정 ID를 사용하도록 승인되었는지 여부를 도메인 소유자가 주장하지 않습니다.
- **SoftFail.** 도메인 소유자는 호스트가 특정 ID를 사용하도록 승인되지 않았다고 믿고 있지만 이를 확고하게 밝히지 않습니다.
- **Fail.** 클라이언트가 특정 ID를 사용하도록 승인되지 않았습니다.
- **TempError.** 확인 중에 일시적인 오류가 발생했습니다.
- **PermError.** 확인 중에 영구적인 오류가 발생했습니다.

메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있을 경우, PRA ID의 Pass 결과를 None으로 다운 그레이드하도록 SIDF Compatible 적합성 레벨을 구성하지 않는 한 어플라이언스는 Pass 결과의 메시

지를 수락합니다. 그런 다음 어플라이언스는 PRA 검사가 None을 반환할 경우에 대해 지정된 SMTP 작업을 수행합니다.

ID 검사에 대한 SMTP 작업을 정의하지 않는 경우 어플라이언스는 Fail을 비롯한 모든 확인 결과를 자동으로 수락합니다.

활성화된 ID 검사에 대해 ID 확인 결과가 REJECT 작업과 일치하는 경우 어플라이언스는 세션을 종료합니다. 예를 들어 관리자는 Fail을 포함하여 HELO ID 확인 결과를 기반으로 메시지를 수신하되, MAIL FROM ID 확인에서 Fail 결과를 받은 메시지는 거부하도록 리스너를 구성합니다. 메시지가 HELO ID 확인에 실패하면 어플라이언스가 해당 결과를 수락하므로 세션이 계속 진행됩니다. 그런 다음 메시지가 MAIL FROM ID 확인에서 실패하면 리스너는 세션을 종료하고 REJECT 작업에 대한 SMTP 응답을 반환합니다.

SMTP 응답은 SPF/SIDF 확인 결과를 기반으로 메시지를 거부할 때 어플라이언스가 반환하는 코드 번호 및 메시지입니다. TempError 결과는 기타 확인 결과와 다른 SMTP 응답을 반환합니다. TempError의 경우 결과 응답 코드는 451이고 기본 메시지 텍스트는 #4.4.3 Temporary error occurred during SPF verification입니다. 다른 모든 확인 결과의 경우 기본 응답 코드는 550이고 기본 메시지 텍스트는 #5.7.1 SPF unauthorized mail is prohibited입니다. TempError 및 기타 확인 결과에 대해 고유한 응답 코드 및 메시지 텍스트를 지정할 수 있습니다.

선택적으로, Neutral, SoftFail 또는 Fail 확인 결과에 대해 REJECT 작업을 수행하는 경우 SPF 계시자 도메인에서 서드파티 응답을 반환하도록 어플라이언스를 구성할 수 있습니다. 기본적으로 어플라이언스는 다음 응답을 반환합니다.

550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>

이러한 SPF/SIDF 설정을 활성화하려면 listenerconfig -> edit 하위 명령을 사용하고 리스너를 선택합니다. Then use the hostaccess -> default subcommand to edit the Host Access Table's default settings. Answer yes to the following prompts to configure the SPF controls:

```
Would you like to change SPF/SIDF settings? [N]> yes
Would you like to perform SPF/SIDF Verification? [Y]> yes
```

Host Access Table에 대해 다음 SPF 제어 설정을 사용할 수 있습니다.

표 17: SPF 제어 설정

적합성 레벨	사용 가능한 SPF 제어 설정
SPF 전용	<ul style="list-style-type: none"> • HELO ID 검사의 수행 여부 • 다음 ID 검사의 결과를 기반으로 수행되는 SMTP 작업 • HELO identity (if enabled) • MAIL FROM Identity • REJECT 작업에 대해 반환된 SMTP 응답 코드 및 텍스트 • 확인 시간제한(초)
SIDF Compatible(SIDF 호환)	<ul style="list-style-type: none"> • HELO ID 검사의 수행 여부 • 메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있을 경우 확인에서 PRA ID의 Pass 결과를 None으로 다운그레이드할지 여부 • 다음 ID 검사의 결과를 기반으로 수행되는 SMTP 작업 • HELO identity (if enabled) • MAIL FROM Identity • PRA Identity • REJECT 작업에 대해 반환된 SMTP 응답 코드 및 텍스트 • 확인 시간제한(초)
SIDF Strict	<ul style="list-style-type: none"> • 다음 ID 검사의 결과를 기반으로 수행되는 SMTP 작업 • MAIL FROM Identity • PRA Identity • SPF REJECT 작업의 경우 반환된 SMTP 응답 코드 및 텍스트 • 확인 시간제한(초)

다음의 예시는 SPF 전용 적합성 수준을 사용하여 SPF/SIDF 확인을 구성하는 사용자를 보여줍니다. 어플라이언스는 HELO ID 검사를 수행하며 None 및 Neutral 확인 결과를 수락하고 나머지는 거부합니다. SMTP 작업에 대한 CLI 프롬프트는 모든 ID 유형에 대해 동일합니다. 사용자는 MAIL FROM ID에 대한 SMTP 작업을 정의하지 않습니다. 어플라이언스는 ID에 대한 모든 확인 결과를 자동으로 수락합니다. 어플라이언스는 모든 REJECT 결과에 대한 기본 거부 코드 및 텍스트를 사용합니다.

예: SPF/SIDF 설정

```

Would you like to change SPF/SIDF settings? [N]> yes
Would you like to perform SPF/SIDF Verification? [N]> yes
What Conformance Level would you like to use?
1. SPF only
2. SIDF compatible
3. SIDF strict
[2]> 1
Would you like to have the HELO check performed? [Y]> y
Would you like to change SMTP actions taken as result of the SPF verification? [N]> y
Would you like to change SMTP actions taken for the HELO identity? [N]> y
What SMTP action should be taken if HELO check returns None?
1. Accept
2. Reject

```



```
[1]> 1
What SMTP action should be taken if HELO check returns Neutral?
1. Accept
2. Reject
[1]> 1
What SMTP action should be taken if HELO check returns SoftFail?
1. Accept
2. Reject
[1]> 2
What SMTP action should be taken if HELO check returns Fail?
1. Accept
2. Reject
[1]> 2
What SMTP action should be taken if HELO check returns TempError?
1. Accept
2. Reject
[1]> 2
What SMTP action should be taken if HELO check returns PermError?
1. Accept
2. Reject
[1]> 2
Would you like to change SMTP actions taken for the MAIL FROM identity? [N]> n
Would you like to change SMTP response settings for the REJECT action? [N]> n
Verification timeout (seconds)
[40]>
```

다음은 리스너의 기본 정책 매개변수에 대해 어떻게 SPF/SIDF 설정이 표시되는지를 보여줍니다.

예: 기본 정책 매개변수의 SPF/SIDF

```
SPF/SIDF Verification Enabled: Yes
Conformance Level: SPF only
Do HELO test: Yes
SMTP actions:
  For HELO Identity:
    None, Neutral: Accept
    SoftFail, Fail, TempError, PermError: Reject
  For MAIL FROM Identity: Accept
SMTP Response Settings:
  Reject code: 550
  Reject text: #5.7.1 SPF unauthorized mail is prohibited.
  Get reject response text from publisher: Yes
  Defer code: 451
  Defer text: #4.4.3 Temporary error occurred during SPF verification.
Verification timeout: 40
```

예 - DMARC 확인 활성화

다음 예에서는 DMARC 확인을 활성화하는 방법을 보여줍니다.

```
mail.example.com> listenerconfig
Currently configured listeners:
1. Listener 1 (on Management, 172.29.181.70) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[ ]> edit
Enter the name or number of the listener you wish to edit.
```

```

[ ]> 1
Name: Listener 1
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[ ]> hostaccess
Default Policy Parameters
=====
Maximum Message Size: 20M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[ ]> default

```

```

Enter the default maximum message size. Add a trailing k for kilobytes, M for megabytes,
or no letter for bytes.
[20M]>
Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>
Enter the maximum number of messages per connection.
[10]>
Enter the maximum number of recipients per message.
[50]>
Do you want to override the hostname in the SMTP banner? [N]>
Would you like to specify a custom SMTP acceptance response? [N]>
Would you like to specify a custom SMTP rejection response? [N]>
Do you want to enable rate limiting per host? [N]>
Do you want to enable rate limiting per envelope sender? [N]>
Do you want to enable Directory Harvest Attack Prevention per host? [Y]>
Enter the maximum number of invalid recipients per hour from a remote host.
[25]>
Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>
Would you like to specify a custom SMTP DHAP response? [Y]>
Enter the SMTP code to use in the response. 550 is the standard code.
[550]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to use SenderBase for flow control by default? [Y]>
Would you like to enable anti-spam scanning? [Y]>
Would you like to enable anti-virus scanning? [Y]>
Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>
Would you like to enable DKIM/DomainKeys signing? [N]>
Would you like to enable DKIM verification? [N]>
Would you like to change SPF/SIDF settings? [N]>
Would you like to enable DMARC verification? [N]> Y
Select the DMARC verification profile to use:
1. DEFAULT
[1]> 1
Would you like to send aggregate reports? [N]> Y
Note: DMARC reports should be DMARC compliant.
Secure delivery is recommended for delivery of DMARC reports.
Please enable TLS support using the `destconfig` command.
Would you like to enable envelope sender verification? [N]> Y
Would you like to specify a custom SMTP response for malformed envelope senders? [Y]>
Enter the SMTP code to use in the response. 553 is the standard code.
[553]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to specify a custom SMTP response for envelope sender domains which do not
resolve? [Y]>
Enter the SMTP code to use in the response. 451 is the standard code.
[451]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to specify a custom SMTP response for envelope sender domains which do not
exist? [Y]>
Enter the SMTP code to use in the response. 553 is the standard code.
[553]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to enable use of the domain exception table? [N]>
Do you wish to accept untagged bounces? [N]>
Default Policy Parameters

```

```

=====
Maximum Message Size: 20M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: Yes
  DMARC Verification Profile: DEFAULT
  Aggregate reports: Yes
Envelope Sender DNS Verification Enabled: Yes
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]>
Name: Listener 1
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>

```

```

Currently configured listeners:
1. Listener 1 (on Management, 172.29.181.70) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
mail.example.com>

```

localeconfig

설명

다국어 설정을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?
(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main body
in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body whenever

```

```

possible.
However, if the disclaimer is encoded differently than the message body, and if imposing a
single encoding
will cause loss of characters, it will be added as an attachment. The system will always
try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit the
message body to
use an encoding that is compatible with the message body as well as the disclaimer. Should
the system try to
re-encode the message body in such a case? [Y]>

```

```

If the disclaimer that is added to the footer or header of the message generates an error
when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added as
an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
content is split into
separate email attachments. Should the system try to ignore such errors when decoding the
message body? [N]>

```

```

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

```

```

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[ ]> mail3.example.com

```

smtpauthconfig

설명

SMTP 인증 발신 및 포워딩 프로필을 구성합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

다음 예에서는 **smtpauthconfig** 명령을 사용하여 서버 "smtp2.example.com:"에 대한 새로운 포워딩 기반 프로필을 생성합니다.

```

mail3.example.com> smtpauthconfig
Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
[ ]> new
Choose the type of profile you wish to create:

```

```

- FORWARD - Create an SMTP Auth forwarding server group profile
- OUTGOING - Create an outgoing SMTP Auth profile
[]> forward
Enter a name for this profile:
[]> forwarding-based
Please begin entering forwarding servers for this group profile.
Enter a hostname or an IP address for the forwarding server:
[]> smtp2.example.com
Enter a port:
[25]>
Choose the interface to use for forwarding requests:
1. Auto
2. Data 1 (192.168.1.1/24: mail3.example.com)
3. Data 2 (192.168.2.1/24: mail3.example.com)
4. Management (192.168.42.42/24: mail3.example.com)
[1]>
Require TLS? (issue STARTTLS) [Y]> y
Enter the maximum number of simultaneous connections allowed:
[10]>
Use SASL PLAIN mechanism when contacting forwarding server? [Y]>
Use SASL LOGIN mechanism when contacting forwarding server? [Y]>
Would you like to enter another forwarding server to this group? [N]>
Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
- EDIT - Edit an existing SMTP Auth profile
- PRINT - List all profiles
- DELETE - Delete a profile
- CLEAR - Delete all profiles
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> created SMTP auth profile
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```



참고 인증된 사용자에게 RELAY HAT 정책이 적용됩니다.

프로필에 둘 이상의 포워딩 서버를 지정할 수 있습니다. SASL 메커니즘인 CRAM-MD5 및 DIGEST-MD5는 Email Security Appliance와 포워딩 서버 간에 지원되지 않습니다.

시스템 설치

systemsetup

설명

최초 시스템 설정 및 시스템 재설치입니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> systemsetup
WARNING: The system setup wizard will completely delete any existing
'listeners' and all associated settings including the 'Host Access Table' -
mail operations may be interrupted.
Are you sure you wish to continue? [Y]> y
Before you begin, please reset the administrator passphrase to a new value.
Old passphrase:
New passphrase:
Retype new passphrase:
*****
You will now configure the network settings for the IronPort C100.
Please create a fully qualified hostname for the IronPort C100 appliance
(Ex: "ironport-C100.example.com"):
[ ]> ironport-C100.example.com
*****
You will now assign an IP address for the "Data 1" interface.
Please create a nickname for the "Data 1" interface (Ex: "Data 1"):
[ ]> Data 1
Enter the static IP address for "Data 1" on the "Data 1" interface? (Ex:
"192.168.1.1"):
[ ]> 192.168.1.1
What is the netmask for this IP address? (Ex: "255.255.255.0" or "0xfffff00"):
[255.255.255.0]>
You have successfully configured IP Interface "Data 1".
*****
Would you like to assign a second IP address for the "Data 1" interface? [Y]> n
What is the IP address of the default router (gateway) on your network?:
[192.168.1.1]> 192.168.2.1
*****
Do you want to enable the web interface on the Data 1 interface? [Y]> y
Do you want to use secure HTTPS? [Y]> y
Note: The system will use a demo certificate for HTTPS.
Use the "certconfig" command to upload your own certificate.
*****
Do you want the IronPort C100 to use the Internet's root DNS servers or would
you like it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use my own DNS servers
[1]> 2
Please enter the IP address of your DNS server.
[ ]> 192.168.0.3
Do you want to enter another DNS server? [N]>
You have successfully configured the DNS settings.
*****
You are now going to configure how the IronPort C100 accepts mail by creating a
"Listener".
Please create a name for this listener (Ex: "MailInterface"):
[ ]> InboundMail
Please choose an IP interface for this Listener.
1. Data 1 (192.168.1.1/24: ironport-C100.example.com)
[1]> 1
Enter the domain names or specific email addresses you want to accept mail for.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
```



```

Separate multiple addresses with commas.
[> example.com, .example.com
Would you like to configure SMTP routes for example.com, .example.com? [Y]> n
Please specify the systems allowed to relay email through the IronPort C100.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[> example.com, .example.com
Do you want to enable filtering based on SenderBase Reputation Service (SBRS)
Scores for this listener? (Your selection will be used to filter all incoming
mail based on its SBRS Score.) [Y]> y
Do you want to enable rate limiting for this listener? (Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a
remote domain.) [Y]> y
Enter the maximum number of recipients per hour to accept from a remote domain.
[> 1000
Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: 1,000
Maximum Recipients Per Hour SMTP Response:
    452 Too many recipients received this hour
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
Would you like to change the default host access policy? [N]> n
Listener InboundMail created.
Defaults have been set for a Public listener.
Use the listenerconfig->EDIT command to customize the listener.
*****
Do you want to use Anti-Spam scanning in the default Incoming Mail policy? [Y]> y
Would you like to enable IronPort Spam Quarantine? [Y]> y
IronPort Anti-Spam configured globally for the IronPort C100 appliance. Use the
policyconfig command (CLI) or Mail Policies (GUI) to customize the IronPort
settings for each listener.
IronPort selected for DEFAULT policy
*****
Do you want to use Anti-Virus scanning in the default Incoming and Outgoing
Mail policies? [Y]> y
1. McAfee Anti-Virus
2. Sophos Anti-Virus
Enter the number of the Anti-Virus engine you would like to use on the default
Incoming and Outgoing Mail policies.
[> 2
Sophos selected for DEFAULT policy
*****
Do you want to enable Outbreak Filters? [Y]> y
Outbreak Filters enabled.

```

```

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below),
meaning that new messages of certain types could be quarantined or will no longer be
quarantined, respectively.
Allow the sharing of limited data with SenderBase? [Y]> y
You have successfully configured Outbreak Filters and SenderBase.
*****
You will now configure system alerts.
Please enter the email address(es) to send alerts.
(Ex: "administrator@example.com")
Separate multiple addresses with commas.
[ ]> administrator@example.com
Would you like to enable IronPort AutoSupport, which automatically emails
system alerts and weekly status reports directly to IronPort Customer Support?
You will receive a complete copy of each message sent to IronPort.
(Recommended) [Y]> y
*****
You will now configure scheduled reporting.
Please enter the email address(es) to deliver scheduled reports to.
(Leave blank to only archive reports on-box.)
Separate multiple addresses with commas.
[ ]> administrator@example.com
*****
You will now configure system time settings.
Please choose your continent:
1. Africa
2. America
...
11. GMT Offset
[11]> 2
Please choose your country:
1. Anguilla
...
47. United States
48. Uruguay
49. Venezuela
50. Virgin Islands (British)
51. Virgin Islands (U.S.)
[ ]> 47
Please choose your timezone:
1. Alaska Time (Anchorage)
...
26. Pacific Time (Los_Angeles)
[ ]> 26
Do you wish to use NTP to set system time? [Y]> y
Please enter the fully qualified hostname or IP address of your NTP server, or
press Enter to use time.ironport.com:
[time.ironport.com]>
*****
Would you like to commit these changes at this time? [Y]> y
Congratulations! System setup is complete.
For advanced configuration, please refer to the User Guide.

```

URL 필터링

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [aggregatorconfig, 311 페이지](#)
- [urllistconfig, 311 페이지](#)

- [webcacheflush, 312 페이지](#)
- [websecurityadvancedconfig, 313 페이지](#)
- [websecurityconfig, 315 페이지](#)
- [websecuritydiagnostics, 316 페이지](#)

aggregatorconfig

설명

Email Security Appliance의 Cisco Aggregator Server에 대한 주소를 구성합니다. 이 서버는 재작성된 URL을 클릭한 엔드 유저 및 각 사용자 클릭과 연결된 작업(허용, 차단, 알 수 없음)의 세부 사항을 제공합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> aggregatorconfig
Choose the operation you want to perform:
- EDIT - Edit aggregator configuration
[]> edit
Edit aggregator address:
[aggregator.organization.com]> org-aggregator.com
Successfully changed aggregator address to : org-aggregator.com
```

urllistconfig

설명

URL 필터링 기능에서 평가하지 않을 URL 화이트리스트를 구성하거나 가져옵니다. 이 목록은 보안 침해 필터에서 사용하지 않습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
> urllistconfig
```

```

No URL lists configured.
Choose the operation you want to perform:
NEW - Create a new URL list-
[ ]> new
Do you want to import a URL list?
[ N ]>
Enter a name for the URL list
[ ]> sample
Enter the URL domains that need to be skipped from scanning for URL Filtering.
Enter one URL domain per line and '.' to finish.
cisco.com
ironport.com/*
*.example.com
10.2.4.5/24
[2001:DB8::1]
URL list sample added.
There are currently 4 URL lists configured.
Choose the operation you want to perform:
- NEW - Create a new URL whitelist.
- EDIT - Modify an existing URL whitelist.
- DELETE - Delete an existing URL whitelist.
[ ]>EDIT
Choose the operation to edit the URL whitelist:
- IMPORT - Import a file into an existing URL whitelist
- EXPORT - Export an existing URL whitelist into a file
- RENAME - Rename an existing URL whitelist
[ ]>IMPORT
Assign new name to the imported list? (By default, name stored in the
file will be applied to the list)
[ N ] > Y
Enter name of the list > new_list
Enter filename to import from > URLfile
NOTE: These files will be stored in /pub/configuration
URL list "new_list" added.

```

webcacheflush

설명

URL 필터링 기능에서 사용하는 캐시를 플러시합니다. Cisco Web Security 서비스와의 통신에 사용하는 인증서를 변경할 경우 이 명령을 사용합니다. 일반적으로 이 명령을 사용할 때는 반드시 Cisco 팀의 지원을 받습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

> webcacheflush
Web Security cache has been flushed.

```

websecurityadvancedconfig

설명

URL 필터링을 위한 고급 설정을 구성합니다.



참고 트러블슈팅을 위해 시간 초과 값을 변경하는 경우를 제외하고, 이 명령을 사용할 때는 반드시 Cisco 팀의 지원을 받습니다.

시간 초과 값은 URL 평판 및 범주를 제공하는 클라우드 서비스와의 통신에 대한 값(초)입니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

배치 형식에 대해서는 CLI 인라인 도움말을 참조하십시오.

예

```
> websecurityadvancedconfig
Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[15]>
Enter the URL cache size (no. of URLs):
[1215000]>
Do you want to disable DNS lookups? [N]>
Enter the maximum number of URLs that should be scanned:
[100]>
Enter the Web security service hostname:
[example.com]>
Enter the threshold value for outstanding requests:
[20]>
Do you want to verify server certificate? [Y]>
Enter the default time-to-live value (seconds):
[30]>
Do you want to include additional headers? [N]>
Enter the default debug log level for RPC server:
[Info]>
Enter the default debug log level for SDS cache:
[Info]>
Enter the default debug log level for HTTP client:
[Info]>
```

예: 단축 URL에 대한 URL 필터링 활성화

다음 예에서는 websecurityadvancedconfig 명령을 사용하여 단축 URL에 대한 URL 필터링을 활성화합니다.

```

maill.example.com> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds: [5]>

Enter the URL cache size (no. of URLs): [810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that should be scanned: [100]>

Enter the Web security service hostname: [v2.sds.cisco.com]>

Enter the threshold value for outstanding requests: [50]>

Do you want to verify server certificate? [Y]>

Do you want to enable URL filtering for shortened URLs? [Y]> yes

For shortened URL support to work, please ensure that ESA is able to connect to the following
domains:
bit.ly, tinyurl.com, ow.ly, tumblr.com, post/ly .....

Enter the default time-to-live value (seconds): [30]>

Do you want to rewrite both the URL text and the href in the message?
Y indicates that the full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server: [Info]>

Enter the default debug log level for URL cache: [Info]>

Enter the default debug log level for HTTP client: [Info]>

```

예: 메시지 첨부 파일의 URL에 대한 스캔 제한 구성

다음 예에서는 `websecurityadvancedconfig` 명령을 사용하여 메시지의 첨부 파일에서 스캔할 수 있는 최대 URL 수를 구성합니다.

```

maill.example.com> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds: [5]>

Enter the URL cache size (no. of URLs): [810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that can be scanned in a message body: [100]>

Enter the maximum number of URLs that can be scanned in the attachments in a message: [25]>

Enter the Web security service hostname: [v2.sds.cisco.com]>

Enter the threshold value for outstanding requests: [50]>

Do you want to verify server certificate? [Y]>

Do you want to enable URL filtering for shortened URLs? [Y]>

```

```

Enter the default time-to-live value (seconds): [30]>

Do you want to rewrite both the URL text and the href in the message?
Y indicates that the full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server: [Info]>

Enter the default debug log level for URL cache: [Info]>

Enter the default debug log level for HTTP client: [Info]>

```

websecurityconfig

설명

URL 필터링의 기본 설정(URL 평판 및 URL 범주 기능)을 구성합니다.

일반적으로 인증서 관리는 자동으로 이루어집니다. Cisco TAC에서 달리 지시하지 않는 한 인증서 설정 프롬프트에서 No를 선택해야 합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 인라인 CLI 도움말을 참조하십시오. 이 명령의 인라인 도움말에 액세스하려면 help 명령을 사용합니다.

예

```

mail.example.com> websecurityconfig
Enable URL Filtering? [N]> y
Do you wish to enable Web Interaction Tracking? [N]> y
Web Interaction Tracking is enabled.
Do you want to whitelist URLs using a URL list? [N]> y
1. urllist1
2. urllist2
3. No URL list
Enter the number of URL list
[1]> 1
URL list 'urllist1' added
mail.example.com> websecurityconfig
URL Filtering is enabled.
URL list 'urllist1' used.
System provided certificate used.
Web Interaction Tracking is enabled.

```

websecuritydiagnostics

설명

URL 필터링과 관련된 진단 통계를 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> websecuritydiagnostics
Cache Size: 254
Cache Hits: 551
Response Time
  Minimum: None
  Average: 0.0
  Maximum: None
DNS Lookup Time
  Minimum: 9.4198775
  Average: 10.1786801765
  Maximum: 10.544356
```

사용자 관리

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [userconfig, 316 페이지](#)
- [passphrase 또는 passwd, 321 페이지](#)
- [last, 322 페이지](#)
- [who, 322 페이지](#)
- [whoami, 323 페이지](#)

userconfig

설명

사용자 계정 및 외부 인증 소스와의 연결을 관리합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 클러스터 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 인라인 CLI 도움말을 참조하십시오. 이 명령의 인라인 도움말에 액세스하려면 help 명령을 사용합니다. 예를 들면 다음과 같습니다.

```
mail.example.com> userconfig help
```

예 - 새 사용자 계정 생성

다음 예에서는 Help Desk User(헬프 데스크 사용자) 역할의 사용자 계정을 새로 생성하는 방법을 보여줍니다.

```
mail.example.com> userconfig
Users:
1. admin - "Administrator" (admin)
External authentication: Disabled
Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.
[ ]> new
Enter your Passphrase to make changes:
Enter the new username.
[ ]> helpdesk
Enter the full name for helpdesk.
[ ]> HELP DESK
Assign a role to "helpdesk":
1. Administrators - Administrators have full access to all settings of the system.
2. Operators - Operators are restricted from creating new user accounts.
3. Read-Only Operators - Read-Only operators may only view settings and status information.
4. Guests - Guest users may only view status information.
5. Technicians - Technician can only manage upgrades and feature keys.
6. Help Desk Users - Help Desk users have access only to ISQ and Message Tracking.
[1]> 6
Would you like to get a system generated passphrase? [N]>
Enter the passphrase for helpdesk
[ ]>
Please enter the new passphrase again:
Users:
1. admin - "Administrator" (admin)
2. helpdesk - "HELP DESK" (helpdesk)
External authentication: Disabled
Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.
[ ]>
```

예 - 외부 인증을 위한 RADIUS 서버 설정

다음 예에서는 외부 인증을 위해 RADIUS 서버를 설정하는 방법을 보여줍니다. RADIUS 서버를 설정하려면 호스트 이름, 공유 암호, 인증 프로토콜로 CHAP 또는 PAP를 사용할지 여부를 입력합니다.

```
mail.example.com> userconfig
Users:
1. admin - "Administrator" (admin)
2. hdesk_user - "Helpdesk User" (helpdesk)
External authentication: Disabled
Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.
[]> external
Choose the operation you want to perform:
- SETUP - Set up global settings.
[]> setup
Do you want to enable external authentication? [N]> Y
Please enter the timeout in seconds for how long the external authentication credentials
will be cached. (Enter '0' to disable expiration of
authentication credentials altogether when using one time passphrases.)
[0]> 30
Choose a mechanism to use:
LDAP is unavailable because no LDAP queries of type EXTERNALAUTH are configured
1. RADIUS
[1]> 1
Configured RADIUS servers:
- No RADIUS servers configured
Choose the operation you want to perform:
- NEW - Add a RADIUS server configuration.
[]> new
Please enter host name or IP address of the RADIUS server:
[]> radius.example.com
Please enter port number of the RADIUS server:
[1812]>
Please enter the shared passphrase:
>
Please enter the new passphrase again.
>
Please enter timeout in seconds for receiving a valid reply from the server:
[5]>
1. CHAP
2. PAP
Select authentication type:
[2]>
Configured RADIUS servers:
Host                Port  Timeout (s)  Auth type
-----
radius.example.com  1812  5            pap
Choose the operation you want to perform:
- NEW - Add a RADIUS server configuration.
- EDIT - Modify a RADIUS server configuration.
- DELETE - Remove a RADIUS server configuration.
```

```
- CLEAR - Remove all RADIUS server configurations.
[]>
```

예: 특정 사용자 역할에 대한 이중 인증 활성화

다음 예에서는 `twofactorauth sub` 명령을 사용하여 특정 사용자 역할에 대한 이중 인증을 활성화합니다.

```
mail.example.com> userconfig

Users:

1. admin - "Administrator" (admin)
2. hdesk_user - "Helpdesk User" (helpdesk)

External authentication: Disabled

Two-Factor Authentication: Disabled

Choose the operation you want to perform:

- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- TWOFACTORAUTH - Configure Two-Factor Authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.

[]> twofactorauth

Choose the operation you want to perform:

- SETUP - Set up global settings.
- PRIVILEGES - Configure Two-Factor Authentication based on User Role Privileges.

[]> setup

Do you want to enable external authentication? [N]> y

Choose the operation you want to perform:

- NEW - Add a two-factor authentication server configuration.
- EDIT - Modify two-factor authentication server configuration.
```

```
- DELETE - Remove a two-factor authentication server configuration.
- CLEAR - Remove all two-factor authentication server configurations.

[> new

Please enter host name or IP address of the RADIUS server:

[> radius.example.com

Please enter port number of the RADIUS server:

[1812]> 1800

Please enter the shared passphrase:

>

Please enter the new passphrase again.

>

Please enter timeout in seconds for receiving a valid reply from the server:

[5]> 10

1. CHAP
2. PAP

Select authentication type:

[2]> 2

Choose the operation you want to perform:

- SETUP - Set up global settings.
- PRIVILEGES - Configure Two-Factor Authentication based on Role Privileges.

[> privileges

Role Privileges:

Choose the operation you want to perform:

1. Add

[> 1

Select Predefined Roles to allow the privileges

1. Administrators
2. Guests
3. Help Desk Users
4. Operators
5. Read-Only Operators
6. Technicians
```

```

Enter the numbers (comma separated) to add privilege.

[ ]> 1

Role Privileges:

Predefined:

Administrators

Choose the operation you want to perform:

1. Add
2. Delete

[ ]>

```

passphrase 또는 passwd

설명

암호를 변경합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 클러스터 모드로 한정됩니다.



참고

passwd 명령은 시스템 모드만 가능한 게스트 사용자가 사용할 수 있어 특별합니다. 게스트 사용자가 클러스터의 어떤 시스템에서 passwd 명령을 실행할 경우 경고 메시지를 인쇄하지 않지만 사용자 모드 변경 없이 클러스터 레벨 데이터를 대상으로 자동으로 작동합니다. 다른 모든 사용자에게 (기타 제한적 컨피그레이션 명령에 따라) 위와 같은 동작이 수행됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```

mail3.example.com> passphrase
Old passphrase: your_old_passphrase
New passphrase: your_new_passphrase
Retype new passphrase: your_new_passphrase
passphrase changed.

```

last

설명

last 명령은 시스템에 최근에 로그인한 사람을 표시합니다. 기본적으로 시스템에 로그인한 모든 사용자를 보여줍니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
elroy.run> last
Username Remote Host Login Time Logout Time Total Time
=====
admin 10.251.23.186 Thu Sep 01 09:14 still logged in 1h 5m
admin 10.251.23.186 Wed Aug 31 14:00 Wed Aug 31 14:01 1m
admin 10.251.16.231 Wed Aug 31 13:36 Wed Aug 31 13:37 0m
admin 10.251.23.186 Wed Aug 31 13:34 Wed Aug 31 13:35 0m
admin 10.251.23.142 Wed Aug 31 11:26 Wed Aug 31 11:38 11m
admin 10.251.23.142 Wed Aug 31 11:05 Wed Aug 31 11:09 4m
admin 10.251.23.142 Wed Aug 31 10:52 Wed Aug 31 10:53 1m
admin 10.251.60.37 Tue Aug 30 01:45 Tue Aug 30 02:17 32m
admin 10.251.16.231 Mon Aug 29 10:29 Mon Aug 29 10:41 11m
shutdown Thu Aug 25 22:20
```

who

설명

who 명령은 CLI를 통해 시스템에 로그인한 모든 사용자, 로그인한 시간, 유효 시간, 사용자가 로그인한 원격 호스트를 나열합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다. 이 명령은 로컬 파일 시스템에 대한 액세스가 필요합니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> who
Username Login Time Idle Time Remote Host What
```

```
=====
admin      03:27PM      0s      10.1.3.201  cli
```

whoami

설명

whoami 명령은 현재 로그인한 사용자의 사용자 이름 및 성명 그리고 사용자가 속한 그룹을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요합니다.

클러스터 관리: 이 명령은 3가지 시스템 모드(클러스터, 그룹, 시스템) 모두에서 사용할 수 있습니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail3.example.com> whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

가상 어플라이언스 관리

- [loadlicense, 323 페이지](#)
- [showlicense, 324 페이지](#)

loadlicense

설명

가상 어플라이언스에 대한 XML 라이선스를 로드합니다. 파일에서 로드하거나 복사하여 붙여넣을 수 있습니다. 자세한 내용은 *Cisco Content Security Virtual Appliance* 설치 설명서 (<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html>)를 참조하십시오.

이 명령은 관리자 또는 운영자 권한이 있는 사용자가 사용할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그인한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

```
mail.example.com> loadlicense
1 Paste via CLI
2 Load from file
How would you like to load a license file?
[1]> 2
Enter the name of the file in /configurations to import:
[]> <filename>
TERMS AND CONDITIONS OF USE
<Terms and conditions>
Do you accept the above license agreement?
[]> y
The license agreement was accepted.
The following feature key have been added:
<feature keys>
```

오류 및 하드웨어 컨피그레이션 오류도 표시될 수 있습니다.

showlicense

설명

현재 가상 어플라이언스 라이선스에 대한 정보를 표시합니다. 추가 세부 사항은 [featurekey](#) 명령을 사용하여 확인할 수 있습니다.

이 명령은 관리자 또는 운영자 권한이 있는 사용자가 사용할 수 있습니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다. 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다.

배치 형식

명령의 구문: showlicense

예

```
mail.example.com> showlicense
company: Example Inc.
org: Widget Division
unit: Portland Data Center
seats: 1000
city: Portland
state: Oregon
country: US
email: mailadmin@example.com
```



```
begin_date: Tue Dec 6 17:45:19 2011
end_date: Mon Sep 1 17:45:19 2014
vln: ABC-123423123
serial: 1003385
```

지리위치

이 섹션은 다음 CLI 명령으로 구성됩니다.

- [geolocationupdate, 325 페이지](#)
- [geolocationstatus, 325 페이지](#)

geolocationupdate

설명

지리위치 목록을 수동으로 업데이트합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원합니다. 자세한 내용은 `help geolocationupdate` 명령을 입력하여 인라인 도움말을 참고하십시오.

예

```
mail3.example.com> geolocationupdate
Requesting update of Geo Countries List.
```

geolocationstatus

설명

지리위치 목록의 현재 버전을 표시합니다.

Usage(사용)

Commit: 이 명령은 'commit'이 필요하지 않습니다.

클러스터 관리: 이 명령은 시스템 모드로 한정됩니다.

배치 명령: 이 명령은 배치 형식을 지원하지 않습니다.

예

예

```
mail3.example.com> geolocationstatus  
  
Component          Version    Last Updated  
Geo Countries List  1.0.48    26 Feb 2017 04:22 (GMT +00:00)
```



색 인

A

기록, CLI [16](#)

C

대/소문자 구분 여부 [15](#)
CLI에서 [15](#)
대괄호 [14](#)
도메인 키 [69](#)
DNS TXT 레코드 [69](#)

D

delivery queue, monitoring [184](#)

G

수신자 반송 [163](#)
모두 [163](#)
호스트 이름별 [163](#)
Envelope From별 [163](#)
숫자 [296](#)
시간당 최대 수신자 수 [296](#)

H

안티스팸 [296](#)
HAT 매개변수 [296](#)
연결 거부 [287](#)
온라인 도움말 [18](#)

J

최대 [296](#)
HAT의 메시지 크기 [296](#)
HAT의 메시지당 수신자 수 [296](#)
HAT의 연결당 메시지 수 [296](#)

K

컨피그레이션 디렉터리 [287](#)
콘텐츠 필터 [220](#)
CLI를 통해 생성 [220](#)

L

텍스트 편집기 [287](#)
텔넷 [13](#)

N

CLI(명령줄 인터페이스) [14, 15, 16](#)
공백 [15](#)
규칙 [14](#)
대/소문자 구분 여부 [15](#)
디폴트 설정 [14](#)
하위 명령 [16](#)
exit [16](#)
history [16](#)
CRAM-MD5 [306](#)
global unsubscribe [185](#)
추가 [185](#)
HAT(Host Access Table) [287](#)
가져오기 및 내보내기 [287](#)
order in [287](#)
LDAP [147](#)
레이저 사용 [147](#)

S

SenderBase [296](#)
SMTP [282, 287](#)
protocol [282](#)
relay [287](#)
SMTP 인증 [306](#)
DIGEST-MD5 [306](#)
SSH [13](#)

