



CLI Reference Guide for AsyncOS 14.3 for Cisco Secure Email Cloud Gateway

First Published: 2022-10-11

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	xxxv
Before you Read this Book	xxxv
Typographic Conventions	xxxv
Additional Resources	xxxvi

CHAPTER 1

CLI Quick Reference Guide	1
CLI Commands (No Commit Required)	1
CLI Commands (Commit Required)	7

CHAPTER 2

Command Line Interface: The Basics	13
Accessing the Command Line Interface (CLI)	13
Factory Default Username and Passphrase	13
Command Line Interface Conventions	14
Command Prompt	14
Command Syntax	15
Select Lists	15
Yes/No Queries	15
Subcommands	15
Escape	16
History	16
Command Completion	16
Configuration Changes	16
General Purpose CLI Commands	17
Committing Configuration Changes	17
Clearing Configuration Changes	18
Quitting the Command Line Interface Session	18

Seeking Help on the Command Line Interface	18
Batch Commands	18
Batch Command Example	18
<hr/>	
CHAPTER 3	The Commands: Reference Examples 21
How to Read the Listing	22
Advanced Malware Protection	22
ampconfig	22
Usage	22
Examples	23
Enabling File Reputation and File Analysis	23
Selecting File Types for File Analysis	24
Configure Email Gateway to Use Public Cloud File Analysis Server	25
(Public Cloud File Analysis Services Only) Configuring Appliance Groups	26
Configure Email Gateway to Use an On-Premises File Analysis Server	26
Configure Email Gateway to Use an On-Premises File Reputation Server	27
Clearing Local File Reputation Cache	28
Configuring Cache Expiry Period for File Reputation disposition values	28
Suppressing File Retrospective Verdict Alerts	29
Configuring Cisco AMP Threat Grid Clustering for File Analysis	30
Configuring Proxy Server Settings for File Analysis	31
ampstatus	32
Description	32
Usage	32
Example	32
Spam and Graymail Management	32
antispamconfig	33
Description	33
Usage	33
Example	33
antispamstatus	34
Description	34
Usage	34
Example	34

antispamupdate	34
Description	34
Usage	34
Example	35
imsandgraymailconfig	35
Description	35
Usage	35
Example	35
graymailstatus	36
Description	36
Usage	37
Example	37
graymailupdate	37
Description	37
Usage	37
Example	37
incomingrelayconfig	37
Description	37
Usage	37
Example: Enabling Incoming Relays - Configuring an Incoming Relay	38
slblconfig	39
Description	39
Usage	40
Batch Format - Import	40
Batch Format	40
Batch Format - Export	40
Example - Importing Safelist/Blocklist Entries	40
Anti-Virus	41
antivirusconfig	41
Description	41
Usage	41
Example	41
Example: Enabling StrongPDF on Sophos Anti-Virus Engine	42
Example: Disabling StrongPDF on Sophos Anti-Virus Engine	43

Viewing Anti-Virus IDE Details	43
antivirusstatus	44
Description	44
Usage	44
Example	44
antivirusupdate	44
Description	44
Usage	45
Example	45
Command Line Management	45
commit	45
Description	45
Usage	45
Example	45
commitdetail	45
Description	45
Usage	46
Example	46
clearchanges or clear	46
Description	46
Usage	46
Example	46
help or h or ?	46
Description	46
Usage	46
Example	47
rollbackconfig	47
Usage	47
Example	47
quit or q or exit	47
Description	47
Usage	47
Example	47
Configuration File Management	48

loadconfig	48
Description	48
Usage	48
Example	48
mailconfig	49
Description	49
Usage	49
Example	49
resetconfig	50
Description	50
Usage	50
Example	50
saveconfig	51
Description	51
Usage	51
Example	51
showconfig	51
Description	51
Usage	51
Example	52
Configuring Email Gateway to Consume External Threat Feeds	52
threatfeedconfig	52
Description	53
Usage	53
Example - Enabling the External Threat Feeds Engine	53
Example - Adding an External Threat Feed Source	53
Example - Adding a SecureX Threat Response Feeds Source	54
threatfeedstatus	56
Description	56
Usage	57
Example - Viewing Current Version of External Threat Feeds Engine	57
threatfeedupdate	57
Description	57
Usage	57

Example - Manually Updating External Threat Feeds Engine 57

Cluster Management 57

- clusterconfig 58
 - Description 58
 - Usage 59
 - Example 59

Data Loss Prevention 59

- dlpstatus 59
 - Usage 60
 - Example 60
- dlpupdate 60
 - Description 60
 - Usage 60
 - Batch Format 60
 - Example 60

Domain Exception List 61

- domainrepconfig 61
 - Description 61
 - Usage 61
 - Example 61

S/MIME Security Services 62

- smimeconfig 62
 - Description 62
 - Usage 62
 - Examples 62

Domain Keys 64

- domainkeysconfig 64
 - Description 64
 - Usage 64
 - Batch Format - Signing Profiles 64
 - Batch Format - Verification Profiles 67
 - Batch Format - Signing Keys 68
 - Batch Format - Search for a Key or Profile 70
 - Batch Format - Global Settings 70

Example: Configuring Domain Keys via the CLI	70
Creating a Sample Domain Keys DNS TXT Record	73
DMARC Verification	74
dmarcconfig	74
Description	74
Usage	74
Batch Format - DMARC Verification Profiles	74
Example	76
DNS	78
dig	79
Description	79
Usage	79
Batch Format	79
Example	80
Example: Verifying TLSA Record of the DNS Server Supporting DNSSEC	80
dnsconfig	81
Description	81
Usage	81
Batch Format	81
Example	83
dnsflush	85
Description	85
Usage	85
Example	85
dnshostprefs	85
Description	85
Usage	85
Example	85
dnslistconfig	86
Description	86
Usage	86
Example	86
dnslisttest	87
Description	87

- Usage 87
- Example 87
- dnsstatus 87
 - Description 87
 - Usage 87
 - Example 87
- Enhanced User Experience using How-Tos Widget 88
 - howtoupdate 88
 - Description 88
 - Usage 88
 - Example 88
 - howtostatus 88
 - Description 88
 - Usage 88
 - Example 88
- General Management/Administration/Troubleshooting 89
 - addressconfig 89
 - Description 89
 - Usage 89
 - Example 89
 - adminaccessconfig 90
 - Description 90
 - Usage 90
 - Batch Format 90
 - Example - Configuring Network Access List 92
 - Example - Configuring Login Banner 93
 - Example - Configuring Web Interface and CLI Session Timeout 94
 - certconfig 95
 - Description 95
 - Usage 95
 - Example - Pasting in a certificate 95
 - Example - Creating a Self-signed Certificate 97
 - Example - Create a Self-signed S/MIME Signing Certificate 98
 - date 99

Description	99
Usage	99
Example	99
daneverify	100
Description	100
Usage	100
Example	100
diagnostic	100
Description	100
Using the diagnostic Command	101
Usage	101
Batch Format	101
Example: Displaying and Clearing Caches	102
Example: Verify Connectivity to Another Mail Server	103
Example: Reset Email Gateway Configuration to the Initial Manufacturer Values	104
Restarting and Viewing Status of Service Engines	104
diskquotaconfig	104
Usage	104
Batch Format	105
Example	105
ecconfig	105
Usage	106
Batch Format	106
Example	106
ecstatus	106
Usage	106
Example	106
ecupdate	107
Usage	107
Batch Format	107
Example	107
encryptionconfig	107
Usage	107
Example	107

encryptionstatus	110
Description	110
Usage	110
Example	110
encryptionupdate	110
Description	110
Usage	111
Example	111
enginestatus	111
Description	111
Usage	111
Example	111
featurekey	112
Description	112
Usage	112
Example	112
featurekeyconfig	113
Description	113
Usage	113
Example	113
generalconfig	113
Description	113
Usage	113
Example - Configure Internet Explorer Compatibility Mode Override	114
healthcheck	114
Description	114
Usage	114
Example	114
healthconfig	114
Description	114
Usage	115
Example	115
ntpconfig	116
Description	116

Usage	116
Example	116
portalregistrationconfig	117
Usage	117
Example	117
reboot	117
Description	117
Usage	117
Example	118
repengstatus	118
Description	118
Usage	118
Example	118
resume	118
Description	118
Usage	118
Example	118
resumedel	119
Description	119
Usage	119
Example	119
resumelister	119
Description	119
Usage	119
Example	119
revert	120
Description	120
Usage	120
Example	120
samlconfig	120
Description	120
Usage	121
Example – Configure New SAML Profile	121
Example – Modifying SAML Profile	123

settime	124
Description	124
Usage	124
Example	124
settz	124
Description	124
Usage	124
Example	125
shutdown	125
Description	125
Usage	125
Example	125
smaconfig	126
Description	126
Usage	126
Example	126
sshconfig	127
Description	127
Usage	127
Examples	127
status	130
Description	130
Usage	130
Example	130
supportrequest	131
Description	131
Usage	131
Example	131
supportrequeststatus	133
Description	133
Usage	133
Example	133
supportrequestupdate	133
Description	133

Usage	133
Example	133
suspend	134
Description	134
Usage	134
Example	134
suspenddel	134
Description	134
Usage	134
Example	134
suspendlistener	135
Description	135
Usage	135
Example	135
tcpservices	135
Description	135
Usage	135
Example	135
techsupport	136
Description	136
Usage	136
Example	136
tlsverify	137
Description	137
Usage	137
Batch Format	137
Example	137
trace	138
Description	138
Usage	138
Example	138
trackingconfig	139
Description	139
Usage	139

Example	140
tzupdate	140
Description	140
Usage	140
Batch Format	140
Example	140
updateconfig	140
Description	140
Usage	141
Examples	141
updatenow	146
Description	146
Usage	146
Batch Format	147
Example	147
version	147
Description	147
Usage	147
Example	147
wipedata	148
Description	148
Usage	148
Example	148
upgrade	148
Description	148
Usage	148
Example	149
Content Scanning	149
contentscannerstatus	149
Usage	149
Example	149
contentscannerupdate	149
Usage	149
Example	150

LDAP	150
ldapconfig	150
Description	150
Usage	150
Example - Creating a New LDAP Server Profile	150
Example - Configuring Global Settings	153
ldapflush	154
Description	154
Usage	154
Example	154
ldaptest	154
Description	154
Usage	154
Example	154
sievechar	155
Description	155
Usage	155
Example	155
Mail Delivery Configuration/Monitoring	156
addresslistconfig	156
Description	156
Usage	156
Batch Format	156
Example	156
aliasconfig	157
Description	157
Usage	157
Batch Format	157
Example	158
archivemessage	160
Description	160
Usage	160
Example	160
altsrchoost	160

Description	160
Usage	160
Example	160
bounceconfig	162
Description	162
Usage	162
Example	162
Applying a Bounce Profile to a Listener	163
bouncerecipients	164
Description	164
Usage	164
Example	165
bvconfig	165
Description	165
Usage	166
Example	166
deleterecipients	167
Description	167
Usage	167
Example	167
Delete All	167
deliveryconfig	168
Description	168
Usage	168
Example	168
delivernow	168
Description	168
Usage	168
Example	169
destconfig	169
Using the destconfig Command	169
Sample Destination Control Table	170
Batch Format	170
Example: Creating a new destconfig Entry	172

Example: Bounce Profile and TLS Settings	173
Example: Inbound “Shock Absorber”	174
Example: Global Settings	175
Example: Enabling TLS Connection with DANE Support	176
hostrate	177
Description	177
Usage	177
Example	177
hoststatus	177
Description	177
Usage	177
Example	178
imageanalysisconfig	179
Description	179
Usage	179
Example	179
oldmessage	180
Description	180
Usage	180
Example	180
rate	180
Description	180
Usage	180
Example	180
redirectrecipients	181
Description	181
Usage	181
Batch Format	181
Example	181
resetcounters	182
Description	182
Usage	182
Example	182
removemessage	182

Description	182
Usage	182
Example	182
showmessage	183
Description	183
Usage	183
Example	183
showrecipients	183
Description	183
Usage	183
Batch Format	183
Example	184
status	184
Usage	184
Example	184
tophosts	185
Description	185
Usage	185
Example	186
topin	186
Description	186
Usage	186
Example	186
unsubscribe	187
Description	187
Usage	187
Example	187
workqueue	188
Description	188
Usage	188
Example	188
Networking Configuration / Network Tools	188
etherconfig	189
Description	189

Usage	189
Example	189
interfaceconfig	190
Description	190
Usage	190
Batch Format	190
Example: Configuring an Interface	191
nslookup	192
Description	192
Usage	193
Example	193
netstat	193
Description	193
Usage	193
Example	194
packetcapture	194
Description	194
Usage	194
Example	194
ping	195
Description	195
Usage	195
Example	196
ping6	196
Description	196
Usage	196
Example	197
routeconfig	197
Description	197
Usage	197
Batch Format	197
Example	198
setgateway	199
Description	199

Usage	199
Example	199
sethostname	200
Description	200
Usage	200
Example	200
smtproutes	200
Description	200
Usage	200
Batch Format	200
Example	201
sslconfig	202
Description	202
Usage	202
Example	202
telnet	209
Description	209
Usage	209
Example	209
traceroute	209
Description	209
Usage	209
Example	210
traceroute6	210
Description	210
Usage	210
Example	210
trailblazerconfig	211
Description	211
Usage	211
Example	212
Outbreak Filters	212
outbreakconfig	212
Description	212

Usage	212
Example	212
outbreakflush	213
Description	213
Usage	213
Example	213
outbreakstatus	213
Description	213
Usage	213
Example	214
outbreakupdate	214
Description	214
Usage	214
Example	214
Policy Enforcement	214
dictionaryconfig	215
Description	215
Usage	215
Example	215
Example - Configuring Maximum Number of Content Dictionaries in Email Gateway	218
exceptionconfig	220
Description	220
Usage	220
Example	220
filters	220
Description	220
Usage	221
Example	221
policyconfig	222
Description	222
Usage	222
Examples	222
quarantineconfig	249
Description	249

Usage	249
Example	250
Users and Quarantines	250
scanconfig	251
Description	251
Usage	251
Example	251
Example: Configuring Message Handling Actions for Unscannable Messages	252
stripheaders	254
Description	254
Usage	254
Example	254
textconfig	255
Description	255
Usage	255
Example	255
Importing Text Resources	256
Exporting Text Resources	257
Logging and Alerts	257
alertconfig	257
Description	257
Usage	257
Example: Creating a New Alert	258
Example: Sending Alerts over TLS	258
displayalerts	260
Description	260
Usage	260
Example	260
findevent	261
Description	261
Usage	261
Example: Search by envelope FROM	261
Example: Search by Message ID	261
Example: Search by Subject	262

Example: Search by envelope TO	262
grep	263
Description	263
Usage	263
Example of grep	263
logconfig	264
Description	264
Usage	264
Example of FTP Push Log Subscription	264
Example of SCP Push Log Subscription	266
Example of Syslog Push Log Subscription	268
Example: Adding a Custom Log Header to Consolidated Event Logs	270
rollovernow	271
Description	271
Usage	271
Example	272
snmpconfig	272
Description	272
Usage	272
Example	272
tail	274
Description	274
Usage	274
Example	275
Reporting	275
reportingconfig	276
Using the reportingconfig command	276
Usage	276
Example: Enabling Reporting Filters (M-Series only)	276
Enabling HAT REJECT Information for Domain Reports (M-Series only)	277
Enabling Timeout Alerts (M-Series only)	277
Enabling Centralized Reporting for an Email Gateway	277
Configure Storage Limit for Reporting Data (C-Series only)	277
Improving Phishing Detection using Service Logs	278

servicelogsconfig	278
Description	279
Usage	279
Example - Enabling Service Logs on Email Gateway	279
Example - Disabling Service Logs on Email Gateway	279
Sender Domain Reputation Filtering	280
sdrconfig	280
Description	280
Usage	280
Example	280
Example – Blocking Messages based on SDR Verdicts at SMTP Conversation Level	281
sdradvancedconfig	282
Description	282
Usage	282
Example	282
sdrdiagnostics	282
Description	283
Usage	283
Example	283
Mailbox Auto Remediation	283
marstatus	283
Description	283
Usage	283
Example	283
marupdate	284
Description	284
Usage	284
Example	284
Smart Software Licensing	284
license_smart	284
Description	285
Usage	285
Example: Configuring Port for Smart Agent Service	285
Example: Enabling Smart Licensing	285

Example: Registering the Email Gateway with the Smart Software Manager	286
Example: Status of Smart Licensing	286
Example: Status Summary of Smart Licensing	287
Example: Setting the Smart Transport URL	287
Example: Requesting Licenses	287
Example: Releasing Licenses	288
Example - Enabling Smart Software Licensing for all Machines in Cluster	288
Example - Registering all Machines in Cluster with Cisco Smart Software Manager	289
Example - Enabling and Registering License Reservation	289
Example - Updating License Reservation	291
Example - Removing License Reservation	291
Example - Disabling License Reservation	292
Example - Enabling License Reservation in Cluster Mode	293
Example - Disabling License Reservation in Cluster Mode	293
Example - Enabling Device Led Conversion Process Manually	294
show_license	294
Description	294
Example: Status of Smart Licensing	294
Example: Status Summary of Smart Licensing	295
smartaccountinfo	295
Description	295
Usage	295
Example: Viewing Smart Account Details	295
SMTP Services Configuration	296
callaheadconfig	296
Description	296
Usage	296
Example	296
Example – Enabling TLS Support for SMTP Call-ahead Recipient Validation	297
listenerconfig	299
Description	299
Usage	300
Batch Format - General listenerconfig	300
Batch Format - HAT	300

Batch Format - RAT	304
Example - Adding a listener	306
Example - Adding a Sender's Country of Origin to a Sender Group	307
Example - Customizing the Host Access Table (HAT) for a listener via Export and Import	311
Example - Enabling Public Key Harvesting and S/MIME Decryption and Verification	317
Example - Advanced HAT Parameters	319
Adding bypass_ca Argument to listenerconfig	321
Example - Configuring SPF and SIDF	321
Example: SPF/SIDF Settings	323
Example: SPF/SIDF in Default Policy Parameters	324
Example - Enable DMARC Verification	324
localeconfig	328
Description	328
Usage	328
Example	328
smtpauthconfig	329
Description	329
Usage	329
Example	329
System Setup	330
systemsetup	330
Description	330
Usage	330
Example	330
URL Filtering	333
aggregatorconfig	333
Description	333
Usage	333
Example	334
retroscannerstatus	334
Description	334
Usage	334
Example	334
retroscannerupdate	334

Description	334
Usage	334
Example	335
urlistconfig	335
Description	335
Usage	335
Example	335
websecurityadvancedconfig	336
Description	336
Usage	336
Batch Format	336
Example	336
websecurityconfig	337
Description	337
Usage	337
Example	337
websecuritydiagnostics	338
Description	338
Usage	338
Example	338
User Management	338
userconfig	338
Description	338
Usage	339
Example - Creating a New User Account	339
Example - Setting Up a RADIUS Server for External Authentication	340
Example - Enabling Two-Factor Authentication for Specific User Role	341
Example – Enabling SAML Authentication	343
Example – Creating New Custom Role for AMP Configuration	344
passphrase or passwd	345
Description	345
Usage	345
Example	346
last	346

- Description 346
 - Usage 346
 - Example 346
- who 346
 - Description 346
 - Usage 346
 - Example 347
- whoami 347
 - Description 347
 - Usage 347
 - Example 347
- Virtual Email Gateway Management 347
 - loadlicense 347
 - Description 347
 - Usage 347
 - Example 348
 - showlicense 348
 - Description 348
 - Usage 348
 - Batch Format 348
 - Example 348
- Geolocation 349
 - geolocationupdate 349
 - Description 349
 - Usage 349
 - Example 349
 - geolocationstatus 349
 - Description 349
 - Usage 349
 - Example 349
- Configuring Cisco Cloud Service Portal Settings and Usage 350
 - cloudserviceconfig 350
 - Description 350
 - Usage 351

Example - Enabling Cisco Cloud Services on Email Gateway	351
Example - Disabling Cisco Cloud Services on Email Gateway	351
Example - Registering Email Gateway with Cisco Cloud Services Portal	352
Example - Automatically Registering Email Gateway with Cisco Cloud Services Portal	352
Example - Deregistering Email Gateway from Cisco Cloud Services Portal	353
Example - Reregistering Email Gateway with Cisco Cloud Services Portal	354
Example - Choosing Cisco Secure Cloud Server to connect Email Gateway to Cisco Cloud Services Portal	354
Example - Enabling Cisco SecureX Threat Response on Email Gateway	355
Example - Disabling Cisco SecureX Threat Response on Email Gateway	356
Example - Enabling CSN on Email Gateway	356
Example - Disabling CSN on Email Gateway	357
Example - Downloading Cisco Cloud Services Certificate and Key from Cisco Talos Intelligence Services Portal	357
Configuring Safe Print Settings on Email Gateway	358
safeprint	358
Description	358
Usage	358
Example	358
Connecting the Email Gateway to Talos Cloud Services	359
talosupdate	359
Description	359
Usage	359
Example	360
talosstatus	360
Description	360
Usage	360
Example	360
Integrating the Email Gateway with Cisco Advanced Phishing Protection	360
eaasconfig	361
Description	361
Usage	361
Example - Registering the Email Gateway	361
eaasupdate	361

Description	361
Usage	362
Example	362
easstatus	362
Description	362
Usage	362
Example	362
Scanning Password-protected Attachments in Messages	362
protectedattachmentconfig	363
Description	363
Usage	363
Example - Enable Scanning of Password-protected Attachments in Incoming and Outgoing Messages	364
Example - Creating User-defined Passphrases to Open Password-protected Attachments	365
Example - Using Only User-defined Passphrases to Open Password-protected Attachments	366
Example - Switching Priority of User-defined Passphrases	368
Example - Editing a User-defined Passphrase	369
Example - Deleting a User-defined Passphrase	371
Configuring OpenID Connect 1.0 on Email Gateway for AsyncOS APIs	372
oidcconfig	373
Description	373
Usage	373
Example - Configuring OpenID Connect for AsyncOS APIs.	373
Example - Deleting OpenID Connect Configuration Settings on Email Gateway	374
Integrating Email Gateway with Cisco Secure Awareness Cloud Service	375
csaconfig	375
Description	375
Usage	375
Example - Enabling Cisco Secure Awareness Cloud Service on Email Gateway	375
Example - Viewing Details of Repeat Clickers List	376
Example - Updating the Repeat Clickers List	376
csastatus	376
Description	377
Usage	377

Example - Displaying Current Version of Cisco Secure Awareness Components	377
csaupdate	377
Description	377
Usage	377
Example - Manually Updating Cisco Secure Awareness Components	377
Integrating Email Cloud Gateway with Cisco Secure Email Threat Defense	378
threatdefenseconfig	378
Description	378
Usage	378
Example - Enabling Threat Defense Connector	378
Example - Disabling Threat Defense Connector	379
Creating a File Hash List	379
filehashlistconfig	379
Description	379
Usage	380
Example - Creating a File Hash List	380



Preface

The instructions in this book are designed for an experienced system administrator with knowledge of networking and email administration.

This chapter contains the following sections:

- [Before you Read this Book, on page xxxv](#)
- [Typographic Conventions, on page xxxv](#)
- [Additional Resources, on page xxxvi](#)

Before you Read this Book



Note If you have already cabled your email gateway to your network, ensure that the default IP address for the email gateway does not conflict with other IP addresses on your network. The IP address assigned to the Management port by the factory is 192.168.42.42. See the “Setup and Installation” chapter in the user guide for your release for more information about assigning IP addresses to the email gateway.

Typographic Conventions

The following table shows the typographic conventions:

Typeface or Symbol	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output.	Please choose an IP interface for this Listener. The sethostname command sets the name of the email gateway.
AaBbCc123	What you type, when contrasted with on-screen computer output.	mail3.example.com> commit Please enter some comments describing your changes: []> Changed the system hostname

Typeface or Symbol	Meaning	Examples
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Command line variable; replace with a real name or value.	Read the <i>QuickStart Guide</i> . The email gateway <i>must</i> be able to uniquely select an interface to send an outgoing packet. Before you begin, please reset your passphrase to a new value. Old passphrase: ironport New passphrase: <i>your_new_passphrase</i> Retype new passphrase: <i>your_new_passphrase</i>

Additional Resources

Documentation

Documentation for your Cisco Secure Email Gateway is available from:

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

Knowledge Base

To access the Knowledge Base for information about Cisco Content Security products, visit:

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

You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, see *Registering for a Cisco Account*.

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general content security issues, as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other users.

Access the Cisco Support Community for Cisco Secure Email Gateway at:

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

Customer Support

Use the following methods to obtain support:

U.S.: Call 1 (408) 526-7209 or Toll-free 1 (800) 553-2447

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

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

Registering for a Cisco Account

Access to many resources on Cisco.com requires a Cisco account.

If you do not have a Cisco.com User ID, you can register for one here:

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

Cisco Welcomes Your Comments

The Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:

contentsecuritydocs@cisco.com

Please include the title of this book and the publication date from the title page in the subject line of your message.



CHAPTER 1

CLI Quick Reference Guide

This chapter contains the following sections:

Use the tables to locate the appropriate CLI command, a brief description and its availability on the C- and M- series platforms.

- [CLI Commands \(No Commit Required\)](#), on page 1
- [CLI Commands \(Commit Required\)](#), on page 7

CLI Commands (No Commit Required)

CLI Command	Description	Platform Availability
ampstatus , on page 32	Display the version of various file reputation and analysis components.	C- Series
antispamstatus , on page 34	Display Anti-Spam status	C- Series
antispamupdate , on page 34	Manually update spam definitions	C- Series
antivirusstatus , on page 44	Display anti-virus status	C- Series
antivirusupdate , on page 44	Manually update virus definitions	C- Series
archivemessage , on page 160	Archives older messages in your queue.	C- Series
bouncerecipients , on page 164	Bounce messages from the queue	C- and M-Series
talosupdate , on page 359	Request for an update of all Talos engine	C- Series
talosstatus , on page 360	Display the current version of Talos Intelligence Services module	C- Series

CLI Command	Description	Platform Availability
clearchanges or clear, on page 46	Clear changes	C- and M-Series
commit, on page 45	Commit changes	C- and M-Series
commitdetail, on page 45	Display detailed information about the last commit	C- Series
contentscannerstatus, on page 149	Display content scanner version information.	C- Series
contentscannerupdate, on page 149	Request manual update of content scanner engine.	C- Series
date, on page 99	Display the current date and time	C- and M- Series
daneverify, on page 100	Checks whether DANE is supported for a specified domain.	C- Series
deleterecipients, on page 167	Delete messages from the queue	C- and M-Series
delivernow, on page 168	Reschedule messages for immediate delivery	C- and M-Series
diagnostic, on page 100	Check RAID disks, network caches, and SMTP connections. Clear network caches.	C- and M-Series
dig, on page 79	Look up a record on a DNS server	C- Series
displayalerts, on page 260	Display the last n alerts sent by the email gateway	C- and M-Series
dlpstatus, on page 59	Version information for DLP Engine	C- Series
dlpupdate, on page 60	Update DLP Engine	C- Series
dnsflush, on page 85	Clear all entries from the DNS cache	C-and M-Series
dnslisttest, on page 87	Test a DNS lookup for a DNS-based list service	C- Series
dnsstatus, on page 87	Display DNS statistics	C- and M-Series
domainreconfig, on page 61	Create a Domain Exception List	C-Series
ecstatus , on page 106	Check the version of the enrollment client that is used to obtain certificates	C-Series
ecupdate , on page 107	Update the enrollment client that is used to obtain certificates	C-Series

CLI Command	Description	Platform Availability
encryptionstatus, on page 110	Shows the version of the PXE Engine and Domain Mappings file	C-Series
encryptionupdate, on page 110	Requests an update to the PXE Engine	C-Series
enginestatus, on page 111	Displays the status and CPU usage of all engines enabled on the email gateway.	C--Series
featurekey, on page 112	Administer system feature keys	C- and M-Series
findevent, on page 261	Find events in mail log files	C- and M-Series
geolocationupdate, on page 349	Manually update the geolocation list.	C- Series
geolocationstatus, on page 349	Displays the current version of the geolocation list.	C-Series
howtoupdate, on page 88	Manually update the How-Tos component	C-Series
howtostatus, on page 88	Displays the current version of the How-Tos component	C-Series
graymailstatus, on page 36	Display the details of existing graymail rules	C-Series
graymailupdate, on page 37	Manually update graymail rules	C-Series
grep, on page 263	Search for text in a log file	C- and M-Series
healthcheck, on page 114	Checks the health of your email gateway.	C-Series
help or h or ?, on page 46	Help	C- and M-Series
hostrate, on page 177	Monitor activity for a particular host	C- and M-Series
hoststatus, on page 177	Get the status of the given hostname	C-and M-Series
last, on page 346	Display who has recently logged into the system	C- and M-Series
ldapflush, on page 154	Flush any cached LDAP results	C- Series
ldaptest, on page 154	Perform a single LDAP query test	C- Series
loadlicense, on page 347	Load a virtual email gateway license	All virtual email gateways
mailconfig, on page 49	Mail the current configuration to an email address	C- and M-Series

CLI Command	Description	Platform Availability
marstatus, on page 283	Display the current version of the MAR component.	C- Series
marupdate, on page 284	Manually update the MAR component.	C- Series
nslookup, on page 192	Query a name server	C- and M-Series
netstat, on page 193	Display network connections, routing tables, and network interface statistics.	C- and M-Series
outbreakflush, on page 213	Clear the cached Outbreak Rules	C- Series
outbreakstatus, on page 213	Display current Outbreak Rules	C- Series
outbreakupdate, on page 214	Update Outbreak Filters rules	C- Series
oldmessage, on page 180	displays a list of old messages in the queue.	C- Series
packetcapture, on page 194	Intercept and display packets being transmitted or received over the network	C- M-Series
passphrase or passwd, on page 345	Change your passphrase	C- and M-Series
ping, on page 195	Ping a network host	C-and M-Series
ping6, on page 196	Ping a network host using IPV6	C- and M-Series
quit or q or exit, on page 47	Quit	C- and M-Series
rate, on page 180	Monitor message throughput	C- and M-Series
reboot, on page 117	Restart the system	C- and M-Series
redirectrecipients, on page 181	Redirect all messages to another relay host	C- Series
removemessage, on page 182	Removes old, undelivered messages from your queue.	C- Series
repengstatus, on page 118	Request version information of Reputation Engine	C- and M-Series
resetconfig , on page 50	Restore the factory configuration defaults	C-and M-Series
resetcounters, on page 182	Reset all of the counters in the system	C-and M-Series
resume, on page 118	Resume receiving and deliveries	C- and M-Series

CLI Command	Description	Platform Availability
resumedel, on page 119	Resume deliveries	C-and M-Series
resumelister, on page 119	Resume receiving	C-and M-Series
revert, on page 120	Revert to a previous release	C- and M-Series
rollovernow, on page 271	Roll over a log file	C- and M-Series
saveconfig, on page 51	Saves the configuration to disk	C- and M-Series
sdrdiagnostics, on page 282	Checks if your Cisco Email Security Gateway is connected to the SDR service	C- Series
settime, on page 124	Manually set the system clock	C- and M-Series
showmessage, on page 183	Displays old undelivered messages in your queue.	C- Series
showconfig, on page 51	Display all configuration values	C- and M-Series
showlicense , on page 348	Display virtual email gateway license information	All virtual email gateways
show_license, on page 294	Shows Smart Licensing status and summary of status.	C-and M-Series
showrecipients, on page 183	Show messages from the queue by recipient host, Envelope From address, or all messages	C- Series
shutdown, on page 125	Shut down the system to power off	C-and M-Series
slblconfig, on page 39	Configure Safelist/Blocklist settings	C-Series
status, on page 130	System status	C- M-Series
supportrequest, on page 131	Send a message to Cisco TAC	C- and M-Series
supportrequeststatus, on page 133	Display Support Request Keywords version information	C- and M-Series
supportrequestupdate, on page 133	Request manual update for Support Request Keywords	C-and M-Series
suspend, on page 134	Suspend receiving and deliveries	C- and M-Series
suspenddel, on page 134	Suspend deliveries	C- and M-Series
suspendlistener, on page 135	Suspend receiving	C-and M-Series
systemsetup, on page 330	First time system setup	C- Series

CLI Command	Description	Platform Availability
tail, on page 274	Continuously display the end of a log file	C- and M-Series
techsupport, on page 136	Allow Cisco TAC to access your system	C- and M-Series
telnet, on page 209	Connect to a remote host	C- and M-Series
threatfeedstatus, on page 56	Display the current version of the ETF engine	C- Series
threatfeedupdate, on page 57	Manually update the ETF engine	C-Series
tlsverify, on page 137	Establish an outbound TLS connection to a remote host and debug any TLS connection issues	C- Series
tophosts, on page 185	Display the top hosts by queue size	C- and M-Series
topin, on page 186	Display the top hosts by number of incoming connections	C- and M-Series
trace, on page 138	Trace the flow of a message through the system	C- and M-Series
traceroute, on page 209	Display the network route to a remote host	C- and M-Series
traceroute6, on page 210	Display the network route to a remote host using IPV6.	C-and M- Series
trailblazerconfig, on page 211	Routes your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface of the email gateway.	C- and M- Series
tzupdate, on page 140	Update timezone rules	C- and M-Series
updatenow, on page 146	Update all components	C-and M-Series
upgrade, on page 148	Install an upgrade	C-and M-Series
version, on page 147	View system version information	C-and M-Series
wipedata, on page 148	Wipe the core files on the disk and check the status of the last coredump operation	C- and M-Series
websecuritydiagnostics, on page 338	View diagnostic statistics for URL filtering	C- and M- Series
who, on page 346	List who is logged in	C-and M-Series
whoami, on page 347	Display your current user id	C-and M-Series
workqueue, on page 188	Display and/or alter work queue pause status	C- Series

CLI Commands (Commit Required)

CLI Command	Description	Platform Availability
addressconfig, on page 89	Configure From: addresses for system generated mail	C- and M- Series
addresslistconfig, on page 156	Configure address lists	C- Series
adminaccessconfig, on page 90	Configure network access list and banner login	C- Series
aggregatorconfig, on page 333	Configure address of the Cisco Aggregator Server	C- Series
alertconfig, on page 257	Configure email alerts	C- and M- Series
aliasconfig, on page 157	Configure email aliases	C- Series
altsrghost, on page 160	Configure Virtual Gateway™ mappings	C- Series
ampconfig, on page 22	Configure Advanced Malware Protection (File reputation and analysis)	C- and M- Series
antispamconfig, on page 33	Configure Anti-Spam policy	C- Series
antivirusconfig, on page 41	Configure anti-virus policy	C- Series
bounceconfig, on page 162	Configure the behavior of bounces	C- and M- Series
bvconfig, on page 165	Configure key settings for outgoing mail, and configure how to handle invalid bounces.	C- Series
callaheadconfig, on page 296	Add, edit, and remove SMTP Call-Ahead profiles	C- and M- Series
certconfig, on page 95	Configure security certificates and keys	C- and M- Series
cloudserviceconfig, on page 350	Configure Cisco Cloud Service Portal settings and usage.	C- and M- Series
clusterconfig, on page 58	Configure cluster related settings	C- Series
csaconfig, on page 375	<ul style="list-style-type: none"> • Enable the Cisco Secure Awareness cloud service on your email gateway. • View details of the Repeat Clickers list. • Update the Repeat Clickers list. 	C- Series

CLI Command	Description	Platform Availability
csastatus, on page 376	Display the current version of the Cisco Secure Awareness components.	C- Series
csaupdate, on page 377	Manually update the Cisco Secure Awareness components.	C- Series
deliveryconfig, on page 168	Configure mail delivery	C- Series
destconfig, on page 169	Configure options for the Destination Controls Table.	C- Series
dictionaryconfig, on page 215	Configure content dictionaries	C- and M- Series
diskquotaconfig, on page 104	Configure disk space	C- and M- Series
dmarconfig, on page 74	Configure DMARC settings	C- Series
dnsconfig, on page 81	Configure DNS setup	C- Series
dnshostprefs, on page 85	Configure IPv4/IPv6 DNS preferences	C- and M- Series
dnslistconfig, on page 86	Configure DNS List services support	C- Series
domainkeysconfig, on page 64	Configure DomainKeys support	C- Series
ecconfig, on page 105	Configure the enrollment client that is used to obtain certificates	C- and M- Series
encryptionconfig, on page 107	Configure email encryption	C- Series
etherconfig, on page 189	Configure Ethernet settings	C- and M- Series
exceptionconfig, on page 220	Configure domain exception table	C- Series
featurekeyconfig, on page 113	Automatically check and update feature keys	C- and M-Series
filters, on page 220	Configure message processing options	C- Series

CLI Command	Description	Platform Availability
filehashlistconfig, on page 379	<ul style="list-style-type: none"> • Create a file hash list for any one of the following supported file hash types – MD5 or SHA-256. • Create a file hash list to configure a content filter to take action on messages that contain attachments that match a particular file hash. • Create a file hash list to use as an exception list for the External Threat Feeds (ETF) feature. 	C- Series
generalconfig, on page 113	Configure browser settings and other general settings	C- and M- Series
healthconfig, on page 114	Configure the threshold of various health parameters of your email gateway	C- and M- Series
imageanalysisconfig, on page 179	Configure the IronPort Image Analysis settings	C- and M- Series
imsandgraymailconfig, on page 35	Configure Cisco Intelligent Multi-Scan (IMS) and graymail detection and safe unsubscribe settings.	C- and M- Series
incomingrelayconfig, on page 37	Configure Incoming Relays	C- Series
interfaceconfig, on page 190	Configure Ethernet IP addresses	C- and M- Series
ldapconfig, on page 150	Configure LDAP servers	C- Series
license_smart, on page 284	Configure smart software licensing feature.	C- and M- Series
listenerconfig, on page 299	Configure mail listeners	C- Series
loadconfig, on page 48	Load a configuration file	C- and M- Series
localeconfig, on page 328	Configure multi-lingual settings	C- Series
logconfig, on page 264	Configure access to log files	C- and M- Series
ntpconfig, on page 116	Configure NTP time server	C- and M- Series

CLI Command	Description	Platform Availability
oidconfig, on page 373	Configure OpenID Connect on your email gateway for AsyncOS APIs. Delete OpenID Connect configuration settings on your email gateway.	C- and M- Series
outbreakconfig, on page 212	Configure Outbreak Filters	C- Series
policyconfig, on page 222	Configure per recipient or sender based policies	C- Series
portalregistrationconfig, on page 117	Set Cisco Talos Email Status Portal registration ID for your email gateway.	C- Series
protectedattachmentconfig, on page 363	Enable scanning of password-protected attachments in incoming or outgoing messages. Create user-defined passphrases to open password-protected attachments in incoming or outgoing messages. Switch priority of user-defined passphrases. Edit user-defined passphrases. Delete user-defined passphrases. View user-defined passphrases.	C- Series
quarantineconfig, on page 249	Configure system quarantines	C- Series
reportingconfig, on page 276	Configure reporting settings	C- and M- Series
rollbackconfig, on page 47	Rollback to one of the previously committed configurations	C- and M- Series
routeconfig, on page 197	Configure IP routing table	C- and M- Series
safeprint, on page 358	Configure safe print settings on your email gateway.	C- and M- Series
samlconfig, on page 120	Configure SAML profiles with the service and identity provider settings	C- and M- Series
scanconfig, on page 251	Configure attachment scanning policy	C- Series
sdrconfig, on page 280	Enable and Configure SDR filtering on your email gateway.	C- Series
sdradvancedconfig, on page 282	Configure advanced parameters when connecting your email gateway to the SDR service.	C- Series

CLI Command	Description	Platform Availability
servicelogsconfig , on page 278	Enable or disable Service Logs on the email gateway.	C-Series
setgateway , on page 199	Set the default gateway (router)	C and M- Series
sethostname , on page 200	Set the name of the machine	C- and M- Series
settz , on page 124	Set the local time zone	C- and M- Series
sievechar , on page 155	Configure characters for Sieve Email Filtering, as described in RFC 3598	C- Series
smartaccountinfo , on page 295	View details of the smart account created in the Cisco Smart Software Manager portal	C- and M- Series
smimeconfig , on page 62	Configure S/MIME functionality	C- and M- Series
smtpauthconfig , on page 329	Configure SMTP Auto profiles	C- Series
smtproutes , on page 200	Set up permanent domain redirections	C- and M- Series
snmpconfig , on page 272	Configure SNMP	C- and M- Series
sshconfig , on page 127	Configure SSH keys	C- and M- Series
sslconfig , on page 202	Configure SSL settings	C- and M- Series
stripheaders , on page 254	Set message headers to remove	C- Series
tcpservices , on page 135	Display information about files opened by processes	C- and M- Series
textconfig , on page 255	Configure text resources	C- Series
threatdefenseconfig , on page 378	Configure advanced message scanning using Threat Defense	C- Series
threatfeedconfig , on page 52	Enable and Configure ETF engine on your email gateway	C- Series
trackingconfig , on page 139	Configure the tracking system	C- and M- Series
unsubscribe , on page 187	Update the global unsubscribe list	C- and M- Series
updateconfig , on page 140	Configure system update parameters	C- Series

CLI Command	Description	Platform Availability
urllistconfig, on page 335	Configure allowed lists of safe URLs.	C-and M- Series
userconfig, on page 338	Manage user accounts and connections to external authentication sources.	C- and M- Series
websecurityadvancedconfig, on page 336	Configure advanced settings for URL filtering	C-and M- Series
websecurityconfig, on page 337	Configure global settings for URL filtering	C- and M- Series



CHAPTER 2

Command Line Interface: The Basics

This chapter contains the following sections:

- [Accessing the Command Line Interface \(CLI\), on page 13](#)
- [Command Line Interface Conventions, on page 14](#)
- [General Purpose CLI Commands, on page 17](#)
- [Batch Commands, on page 18](#)

Accessing the Command Line Interface (CLI)

The Command Line Interface is accessible via SSH or Telnet on IP interfaces that have been configured with these services enabled, or via terminal emulation software on the serial port. By factory default, SSH and Telnet are configured on the Management port. Use the `interfaceconfig` command to disable these services.

Access to the CLI varies depending on the management connection method chosen while setting up the email gateway. The factory default username and passphrase are listed next. Initially, only the admin user account has access to the CLI. You can add other users with differing levels of permission after you have accessed the command line interface for the first time via the admin account. The system setup wizard asks you to change the passphrase for the admin account. The passphrase for the admin account can also be reset directly at any time using the `passphrase` command.

To connect via Ethernet: Start an SSH or Telnet session with the factory default IP address 192.168.42.42. SSH is configured to use port 22. Telnet is configured to use port 23. Enter the username and passphrase below.

To connect via a Serial connection: Start a terminal session with the communication port on your personal computer that the serial cable is connected to. See the “Setup and Installation” chapter for more information. Enter the username and passphrase below.

Log in to the email gateway by entering the username and passphrase below.

Factory Default Username and Passphrase

- Username: **admin**
- Passphrase: **ironport**

For example:

```
login: admin
passphrase: ironport
```

Command Line Interface Conventions

This section describes the rules and conventions of the AsyncOS CLI.

Command Prompt

The top-level command prompt consists of the fully qualified hostname, followed by the greater than (>) symbol, followed by a space. For example:

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

If the email gateway has been configured as part of a cluster with the Centralized Management feature, the prompt in the CLI changes to indicate the current mode. For example:

```
(Cluster Americas) >
```

or

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

See “Centralized Management” in the user guide for more information.

When running commands, the CLI requires input from you. When the CLI is expecting input from you, the command prompt shows the default input enclosed in square brackets ([]) followed by the greater than (>) symbol. When there is no default input, the command prompt brackets are empty.

For example:

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

When there is a default setting, the setting is displayed within the command prompt brackets. For example:

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

When a default setting is shown, typing Return is equivalent to typing the default:

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

Command Syntax

When operating in the interactive mode, the CLI command syntax consists of single commands with no white spaces and no arguments or parameters. For example:

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

Select Lists

When you are presented with multiple choices for input, some commands use numbered lists. Enter the number of the selection at the prompt.

For example:

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

Yes/No Queries

When given a yes or no option, the question is posed with a default in brackets. You may answer **Y**, **N**, **Yes**, or **No**. Case is not significant.

For example:

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

Subcommands

Some commands give you the opportunity to use subcommands. Subcommands include directives such as **NEW**, **EDIT**, and **DELETE**. For the **EDIT** and **DELETE** functions, these commands provide a list of the records previously configured in the system.

For example:

```
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.
[ ]>
```

Within subcommands, typing Enter or Return at an empty prompt returns you to the main command.

Escape

You can use the Control-C keyboard shortcut at any time within a subcommand to immediately exit return to the top level of the CLI.

History

The CLI keeps a history of all commands you type during a session. Use the Up and Down arrow keys on your keyboard, or the Control-P and Control-N key combinations, to scroll through a running list of the recently-used commands.

```
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)
```

Command Completion

The command-line interface supports command completion. You can type the first few letters of some commands followed by the Tab key, and the CLI completes the string for unique commands. If the letters you entered are not unique among commands, the CLI “narrows” the set. For example:

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

For both the history and file completion features of the CLI, you must type Enter or Return to invoke the command.

Configuration Changes

You can make configuration changes while email operations proceed normally.

Configuration changes will not take effect until you complete the following steps:

Procedure

-
- Step 1** Issue the commit command at the command prompt.
 - Step 2** Give the commit command the input required.
 - Step 3** Receive confirmation of the commit procedure at the CLI.
-

What to do next

Changes to configuration that have not been committed will be recorded but not put into effect until the commit command is run.



Note Not all commands require the commit command to be run. See [CLI Quick Reference Guide, on page 1](#) for a summary of commands that require commit to be run before their changes take effect.

Exiting the CLI session, system shutdown, reboot, failure, or issuing the clear command clears changes that have not yet been committed.

General Purpose CLI Commands

This section describes the commands used to commit or clear changes, to get help, and to quit the command-line interface.

Committing Configuration Changes

The commit command is critical to saving configuration changes to the email gateway. Many configuration changes are not effective until you enter the commit command. (A few commands do not require you to use the commit command for changes to take effect. The commit command applies configuration changes made since the last commit command or the last clear command was issued. You may include comments up to 255 characters. Changes are not verified as committed until you receive confirmation along with a timestamp.

Entering comments after the commit command is optional.

```
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
```



Note To successfully commit changes, you must be at the top-level command prompt. Type Return at an empty prompt to move up one level in the command line hierarchy.

Clearing Configuration Changes

The clear command clears any configuration changes made since the last commit or clear command was issued.

```
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>
```

Quitting the Command Line Interface Session

The quit command logs you out of the CLI application. Configuration changes that have not been committed are cleared. The quit command has no effect on email operations. Logout is logged into the log files. (Typing exit is the same as typing quit.)

```
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
```

Seeking Help on the Command Line Interface

The help command lists all available CLI commands and gives a brief description of each command. The help command can be invoked by typing either help or a single question mark (?) at the command prompt.

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

Batch Commands

AsyncOS includes support for batch command formats that allow you to execute certain CLI commands using a new, single-line CLI format. This format reduces the number of inputs required to complete tasks and provides a mechanism allowing you to easily automate common configuration tasks. Batch commands also allow you to issue commands remotely using an SSH client. This enables you to easily script CLI commands and execute them on multiple email gateways at one time.

Not all commands have a batch equivalent, but all batch commands can be executed as non-batch commands.

Batch command syntax is dependent on the specific command being used. Please see the appropriate CLI example in [The Commands: Reference Examples, on page 21](#) for more information about syntax specific to that command.

Batch Command Example

In the following example, the sendergroup REDLIST is created. It is then associated with the policy THROTTLED, and then the sender 'possible_spammer.com' is added to the sender group.

To execute this action using the CLI:

```
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 blocked list queries such as `dnslist[query.blocked list.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.

To perform the same action using a CLI batch command:

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



CHAPTER 3

The Commands: Reference Examples

This chapter contains the following sections:

- [How to Read the Listing, on page 22](#)
- [Advanced Malware Protection, on page 22](#)
- [Spam and Graymail Management, on page 32](#)
- [Anti-Virus, on page 41](#)
- [Command Line Management, on page 45](#)
- [Configuration File Management, on page 48](#)
- [Configuring Email Gateway to Consume External Threat Feeds, on page 52](#)
- [Cluster Management, on page 57](#)
- [Data Loss Prevention, on page 59](#)
- [Domain Exception List, on page 61](#)
- [S/MIME Security Services, on page 62](#)
- [Domain Keys, on page 64](#)
- [DMARC Verification, on page 74](#)
- [DNS, on page 78](#)
- [Enhanced User Experience using How-Tos Widget , on page 88](#)
- [General Management/Administration/Troubleshooting, on page 89](#)
- [Content Scanning, on page 149](#)
- [LDAP, on page 150](#)
- [Mail Delivery Configuration/Monitoring, on page 156](#)
- [Networking Configuration / Network Tools, on page 188](#)
- [Outbreak Filters, on page 212](#)
- [Policy Enforcement, on page 214](#)
- [Logging and Alerts, on page 257](#)
- [Reporting, on page 275](#)
- [Improving Phishing Detection using Service Logs, on page 278](#)
- [Sender Domain Reputation Filtering, on page 280](#)
- [Mailbox Auto Remediation, on page 283](#)
- [Smart Software Licensing, on page 284](#)
- [SMTP Services Configuration, on page 296](#)
- [System Setup, on page 330](#)
- [URL Filtering , on page 333](#)
- [User Management, on page 338](#)

- [Virtual Email Gateway Management](#) , on page 347
- [Geolocation](#), on page 349
- [Configuring Cisco Cloud Service Portal Settings and Usage](#), on page 350
- [Configuring Safe Print Settings on Email Gateway](#), on page 358
- [Connecting the Email Gateway to Talos Cloud Services](#) , on page 359
- [Integrating the Email Gateway with Cisco Advanced Phishing Protection](#), on page 360
- [Scanning Password-protected Attachments in Messages](#), on page 362
- [Configuring OpenID Connect 1.0 on Email Gateway for AsyncOS APIs](#), on page 372
- [Integrating Email Gateway with Cisco Secure Awareness Cloud Service](#), on page 375
- [Integrating Email Cloud Gateway with Cisco Secure Email Threat Defense](#), on page 378
- [Creating a File Hash List](#), on page 379

How to Read the Listing

For each command, there is a description and at least one example of the command being used. The Usage section specifies the following command attributes:

Procedure

- Step 1** Does the command require a commit command to be implemented on the email gateway?
- Step 2** Is the command restricted to a particular mode (cluster, group, or machine).?
- Step 3** Does the command permit a batch format?

For more information about Centralized Management, see *User Guide for AsyncOS for Cisco Secure Email Gateway* .

For more information about batch formats, please see [Command Line Interface: The Basics](#), on page 13.

Advanced Malware Protection

ampconfig

Configure file reputation filtering and file analysis. Do not modify advanced options without guidance from Cisco TAC.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For details, see the inline help by typing the command: help ampconfig .

Examples

Enabling File Reputation and File Analysis

```
mail.example.com> ampconfig

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.

[]>
```

Selecting File Types for File Analysis

```

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.
[]>

```

Configure Email Gateway to Use Public Cloud File Analysis Server

```

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.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]>
...
```

(Public Cloud File Analysis Services Only) Configuring Appliance Groups

To allow all appliances in your organization to view file analysis result details in the cloud for files sent for analysis from any appliance in your organization, you need to join all appliances to the same appliances group.

For more information, see the “File Reputation Filtering and File Analysis” chapter in the user guide.

```
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.
[ ]> 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.
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESettings - Configure the cache settings for AMP.
[ ]>
```



Note If you want to modify the Appliance Group ID/Name, use the `SETGROUP` command. You can view the appliances added to a Appliance Group using the `VIEWGROUP` subcommand.

Configure Email Gateway to Use an On-Premises File Analysis Server

```
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.
[ ]>

```

Configure Email Gateway to Use an On-Premises File Reputation Server

```

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)

```

Clearing Local File Reputation Cache

```

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-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+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.
[ ]>

```

Clearing Local File Reputation Cache

```

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.
[ ]> 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.
[ ]> clearcache

```

Configuring Cache Expiry Period for File Reputation disposition values

In the following example, the `modifytimeout` sub command is used to configure the cache expiry period for malicious files.



Note The cache expiry period must be a value from 15 minutes to 7 days.

```
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
```

Suppressing File Retrospective Verdict Alerts

```
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
```

Configuring Cisco AMP Threat Grid Clustering for File Analysis

```

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.
- []>

Configuring Proxy Server Settings for File Analysis

```
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?
```

```
[20]>
```

Choose a file reputation server:

1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud

[1]>

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

```
Enter heartbeat interval?
```

```
[15]>
```

```
Proxy server detail:
```

```
Server : 10.8.6.7
```

```
Port : 3128
```

```
User : testuser1
```

```
Passphrase: xxxxxx
```

```
Do you want to change proxy detail [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. EUROPE (https://panacea.threatgrid.eu)
3. Private analysis cloud

[1]>

```
Use Existing File Reputation Proxy? [N]> no
```

```
Proxy server detail:
```

```
Server: 10.8.6.7
```

```

Port: 3128
User: testuser1
Password: xxxxxxxx

Do you want to change proxy detail [N]> yes

Enter proxy server url?
[10.8.6.7]> 10.8.7.5

Enter proxy port?
[3128]> 3230

Enter Username?
[testuser1]> testuser2

Edit passphrase []? [N]> no

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.
[]>

```

ampstatus

Description

Display the version of various Advanced Malware Protection (file reputation and analysis) components.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```

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

```

Spam and Graymail Management

This section contains the following commands:

antispamconfig

Description

Configure anti-spam policy.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

The following examples demonstrates the configuration for Anti-Spam functionality.

```
mail3.example.com> antispamconfig

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]>
Choose Scanning Profile
1. Normal - Scanning profile used to block spam with small potential for false positives.
2. Aggressive - Scanning profile used to block spam that has more impact on spam detection than the Normal profile with a larger potential for false positives.

If you have changed the global scanning profile settings, you must review the Anti-Spam policy thresholds (Mail Policies > Incoming/Outgoing Mail Policies > Anti-Spam) to produce satisfactory results.
If you have changed the scanning profile setting from Normal to Aggressive, you need to reset the mail policy threshold values to the default values to avoid undesirable false positives.
For Aggressive scanning profile, it is recommended to tune the policy threshold values to smaller increments compared to the threshold values of the Normal scanning profile.
IronPort Anti-Spam scanning is now enabled on the system.
Please note: You must issue the policyconfig command or Mail Policies (GUI) to configure Cisco IronPort scanning behavior for default and custom 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

Description

Display anti-spam status.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
mail3.example.com> antispamstatus
Choose the operation you want to perform:
- IRONPORT - Display IronPort Anti-Spam 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

Description

Manually request an immediate update of Anti-Spam rules and related CASE components. This also includes the Anti-Spam rules and CASE components used by Intelligent Multi-Scan (IMS), but not for the third-party anti-spam engines used by IMS.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command does not support a batch format.

Example

```
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

[]> ironport
Requesting check for new CASE definitions
```

imsandgraymailconfig

- [Description, on page 35](#)
- [Usage, on page 35](#)
- [Example, on page 35](#)

Description

Configure the Cisco Intelligent Multi-Scan (IMS) and Graymail Detection and Safe Unsubscribe settings.



Note

- To configure the threshold for message scanning by Cisco Intelligent Multi-Scan and Graymail Detection and Safe Unsubscribing, use the `imsandgraymailconfig > globalconfig` sub command. These global configuration settings are common for both Cisco Intelligent Multi-Scan and Graymail Detection and Safe Unsubscribing.
- To configure policy settings for graymail detection and safe unsubscribing, use the `policyconfig` command. For more information, see [Create an Incoming Policy to Drop the Messages Identified as Bulk Email or Social Network Email, on page 240](#).

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format for graymail configuration. For more details, see the inline help by typing the command: `help imsandgraymailconfig`.

Example

The following examples demonstrates the configurations for Graymail Detection and Safe Unsubscribing and Intelligent Multi-Scan.

```
mail3.example.com> imsandgraymailconfig

Choose the operation you want to perform:
- GRAYMAIL - Configure Graymail Detection and Safe Unsubscribe settings
- MULTISCAN - Configure IronPort Intelligent Multi-Scan.
- GLOBALCONFIG - Common Global Configuration settings
[]> graymail
Graymail Detection: Disabled
```

```

Choose the operation you want to perform:
- SETUP - Configure Graymail.
[]> setup
Would you like to use Graymail Detection? [Y]> y

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]> 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.

[]> multiscan
IronPort Intelligent Multi-Scan: Disabled

Choose the operation you want to perform:
- SETUP - Edit Intelligent Multi-Scan settings.
[]> setup

IronPort Intelligent Multi-Scan scanning: Disabled
Would you like to use IronPort Intelligent Multi-Scan scanning? [Y]> y
Would you like to enable regional scanning? [N]> n

Intelligent Multi-Scan scanning is now enabled on the system. Please note: you must issue
the 'policyconfig' command (CLI) or Mail Policies (GUI) to configure
Intelligent Multi-Scan scanning behavior for default and custom Incoming and Outgoing Mail
Policies. This is recommended for your DEFAULT policy.

IronPort Intelligent Multi-Scan: Enabled

[]> globalconfig

Choose the operation you want to perform:
- SETUP - Configure Common Global settings
[]> setup

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]>

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

```

graymailstatus

Description

Display the details of the existing graymail rules.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```
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

Description

Manually request update of the graymail rules.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

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

incomingrelayconfig

Description

Use the **incomingrelayconfig** command to enable and configure the Incoming Relays feature. In the following examples, the Incoming Relays feature is first enabled, and then two relays are added, one is modified, and one is deleted.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example: Enabling Incoming Relays - Configuring an Incoming Relay

```

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
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
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
to parse:      Match
-----      -----      -----
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:
[]> 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
[]> 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
[]> 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
[]>

```

sblconfig

Description

Configure End-User Safelist/Blocklist.



Note Safelists/Blocklists must be enabled on the appliance via the GUI in order to run this command.

Usage

Commit: This command does not require a 'commit'.

Batch Command: This command supports a batch format.

Batch Format - Import

Batch Format

Replaces all entries in the End-User Safelist/Blocklist with entries present in the specified file.

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

- filename - Name of the file that has to be imported. The file must be in the /configuration directory on the email gateway.
- ignore invalid entries - Whether to ignore invalid entries or not. Either 'Yes' or 'No.'

Batch Format - Export

Exports all entries in the End-User Safelist/Blocklist to a file the email gateway.

```
slblconfig export
```

The email gateway saves a .CSV file to the /configuration directory using the following naming convention:

slbl<timestamp><serial number>.csv.

Example - Importing Safelist/Blocklist Entries

```
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.
[ ]>
```

Anti-Virus

This section contains the following CLI commands:

antivirusconfig

Description

Configure anti-virus policy.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In the following example, the `antivirusconfig` command is used to enable Sophos virus scanning on the system and set the time-out value to 60 seconds. To configure the update server, update interval, and optional proxy server, see [updateconfig](#), on page 140.



Note The first time you invoke the `antivirusconfig` command, you may be presented with a license agreement, if you did not accept the license during the `systemsetup` command. If you do not accept the license agreement, the Sophos virus scanning engine will not be enabled on the email gateway.

```
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
```

Example: Enabling StrongPDF on Sophos Anti-Virus Engine

```

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.
[ ]>

```

Example: Enabling StrongPDF on Sophos Anti-Virus Engine

In the following example, you can use the `antivirusconfig > PDF` sub command to enable the strongPDF option on the Sophos Anti-Virus engine in your email gateway.

```

mail.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.
- PDF - Scanning of PDF files by Sophos Anti-Virus
engine.
[ ]> pdf

Currently, clean files that are corrupted because
of 'EOF missing,'etc. are marked as 'Clean' by the
Sophos Anti-Virus engine.

Do you want to mark a clean file that is corrupted
as clean? [Y]> no

Sophos Anti-Virus: Enabled

Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
- PDF - Scanning of PDF files by Sophos Anti-Virus engine.
[ ]>

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

mail.example.com> commit

Please enter some comments describing your changes:
[ ]>

Do you want to save the current configuration for
rollback? [Y]>

Changes committed: Tue May 12 17:59:55 2020 GMT

```


Example: Disabling StrongPDF on Sophos Anti-Virus Engine

In the following example, you can use the `antivirusconfig > PDF` sub command to disable the strongPDF option on the Sophos Anti-Virus engine in your email gateway.

```
mail.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.
- PDF - Scanning of PDF files by Sophos
Anti-Virus engine.
[]> pdf

Currently, clean files that are corrupted
because of 'EOF missing,'etc. are marked as
'Unscannable' by the Sophos Anti-Virus engine.

Do you want to mark a clean file that is
corrupted as clean? [N]> yes

Sophos Anti-Virus: Enabled

Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
- PDF - Scanning of PDF files by Sophos Anti-Virus engine.
[]>

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

mail.example.com> commit

Please enter some comments describing your
changes:
[]>

Do you want to save the current configuration
for rollback? [Y]>

Changes committed: Tue May 12 18:13:46 2020 GMT
```

Viewing Anti-Virus IDE Details

AsyncOS provides detailed status on the specific anti-virus signature files (IDE files) that have been downloaded by the email gateway. You can access these details using the `antivirusconfig -> detail` subcommand. For example:

```
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
'Oddbob-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

Description

Display Anti-Virus status.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

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

Description

Manually update virus definitions.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command does not support a batch format.

Example

```
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>
```

Command Line Management

This section contains the following CLI commands:

commit

Description

Commit changes. Entering comments after the commit command is optional.

Usage

Commit: N/A

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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
```

commitdetail

Description

Display detailed information about the last commit.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

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

clearchanges or clear

Description

The **clear** command clears any configuration changes made since the last commit or clear command was issued.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```
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 or h or ?

Description

The **help** command lists all available CLI commands and gives a brief description of each command. The **help** command can be invoked by typing either help or a single question mark (?) at the command prompt.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

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

rollbackconfig

The **rollbackconfig** command allows you to rollback to one of the previously committed 10 configurations.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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 or q or exit

Description

The **quit** command logs you out of the CLI application. Configuration changes that have not been committed are cleared. The **quit** command has no effect on email operations. Logout is logged into the log files. (Typing exit is the same as typing quit.)

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```
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
```

Configuration File Management

This section contains the following CLI commands:

loadconfig

Description

Load a configuration file.



Note Loading configuration on clustered machines is supported only using GUI. For instructions, see *User Guide for AsyncOS for Cisco Secure Email Gateway*.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

In this example, a new configuration file is imported from a local location.

```
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
```

In this example, a new configuration file is pasted directly at the command line. (Remember to type Control-D on a blank line to end the paste command.) Then, the system setup wizard is used to change the default hostname, IP address, and default gateway information. Finally, the changes are committed.

```
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

Description

To test the configuration, you can use the **mailconfig** command immediately to send a test email containing the system configuration data you just created with the **systemsetup** command.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```

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.

```

Send the configuration to a mailbox to which you have access to confirm that the system is able to send email on your network.



Note For enhanced security, if encryption of sensitive data in the email gateway is enabled in fipsconfig command, you cannot use Plain passwords option.

resetconfig

Description

When physically transferring the email gateway, you may want to start with factory defaults. The `resetconfig` command resets *all* configuration values to factory defaults. This command is extremely destructive, and it should only be used when you are transferring the unit or as a last resort to solving configuration issues. It is recommended you run the `systemsetup` command after reconnecting to the CLI after you have run the `resetconfig` command.



Note The `resetconfig` command only works when the email gateway is in the offline state. When the `resetconfig` command completes, the email gateway is automatically returned to the online state, even before you run the `systemsetup` command again. If mail delivery was suspended before you issued the `resetconfig` command, the mail will attempt to be delivered again when the `resetconfig` command completes.



Danger The `resetconfig` command will return all network settings to factory defaults, potentially disconnecting you from the CLI, disabling services that you used to connect to the email gateway (FTP, Telnet, SSH, HTTP, HTTPS), and even removing additional user accounts you created with the `userconfig` command. Do not use this command if you are not able to reconnect to the CLI using the Serial interface or the default settings on the Management port through the default Admin user account.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
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

Description

The **saveconfig** command saves the configuration file with a unique filename to the configuration directory.



Note If you are on a clustered environment, this command saves the complete cluster configuration. To run this command on a clustered machine, change your configuration mode to cluster.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

In the following example, the passphrases in the configuration file is encrypted and saved in the configuration directory.

```
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.
```



Note For enhanced security, if encryption of sensitive data in the email gateway is enabled in fipsconfig command, you cannot use Plain passwords option.

showconfig

Description

The **showconfig** command prints the current configuration to the screen.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

In the following example, the configuration is displayed on CLI and the passphrases in the configuration are encrypted.

```
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.]
```



Note For enhanced security, if encryption of sensitive data in the email gateway is enabled in `fipsconfig` command, you cannot use Plain passwords option.

Configuring Email Gateway to Consume External Threat Feeds

- [threatfeedconfig](#), on page 52
- [threatfeedstatus](#), on page 56
- [threatfeedupdate](#), on page 57

threatfeedconfig

- [Description](#), on page 53
- [Usage](#), on page 53
- [Example - Adding an External Threat Feed Source](#), on page 53
- [Example - Adding a SecureX Threat Response Feeds Source](#), on page 54

Description

The `threatfeedconfig` command is used to

- Enable the ETF engine in your email gateway.
- Configure an ETF source in your email gateway.
- Configure a SecureX Thread Response feeds source in your email gateway.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example - Enabling the External Threat Feeds Engine

In the following example, you can use the `setup` subcommand to enable the ETF engine on your email gateway.

```
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.
```

```
[ ]>
```

Example - Adding an External Threat Feed Source

In the following example, you can use the `sourceconfig` subcommand to add an ETF source on your email gateway.

```
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.
```

Example - Adding a SecureX Threat Response Feeds 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:
[]> guest.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.

```

Example - Adding a SecureX Threat Response Feeds Source

In the following example, you can use the `threatfeedconfig> sourceconfig sub` command to add a SecureX Threat Response feeds source in your email gateway.



Note The SecureX Threat Response feeds source is different from a typical TAXII feeds source. However, to enable polling of observables from the SecureX Threat Response server, you must map the SecureX Threat Response feed URL to the following TAXII source parameters.

- Hostname
- Polling Path
- Collection Name

For Example: The following is a sample SecureX Threat Response feed URL created in the SecureX Threat Response portal.

```
<https://private.intel.amp.cisco.com/ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view.txt?s=e8f3f519-9170-4b76-8b58-bda0be540ff3>
```

You can map the sample SecureX Threat Response feed URL details to the following TAXII source parameters:

- **Hostname** - consists of the “*private.intel.amp.cisco.com*” part of the SecureX Threat Response feed URL.
- **Polling Path** -: consists of the “*/ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view*” part of the SecureX Threat Response feed URL.



Note Do not include the “.txt” part of the SecureX Threat Response feed URL in the Polling Path.

- **Collection Name** - consists of “*e8f3f519-9170-4b76-8b58-bda0be540ff3*” part of the SecureX Threat Response feed URL.

Using the above example, you can configure the ‘Hostname,’ ‘Polling Path,’ and ‘Collection Name’ parameters.

```
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:
[> securex_ctr_source

Enter a description for the external threat feed source (optional):
[> SecureX Threat Response source

Enter the host name for the external threat feed source:
[> private.intel.amp.cisco.com

Enter the polling path for the external threat feed source:
[> /ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view

Enter the collection name for the external threat feed source:
[> e8f3f519-9170-4b76-8b58-bda0be540ff3

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]>

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]>

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]>

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

securex_ctr_source successfully added.

```

threatfeedstatus

- [Description, on page 56](#)
- [Usage, on page 57](#)
- [Example - Viewing Current Version of External Threat Feeds Engine, on page 57](#)

Description

The `threatfeedstatus` command is used to display the current version of the ETF engine.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example - Viewing Current Version of External Threat Feeds Engine

In the following example, you can use the `threatfeedstatus` command to view the current version of the ETF engine.

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

threatfeedupdate

- [Description, on page 57](#)
- [Usage, on page 57](#)
- [Example - Manually Updating External Threat Feeds Engine, on page 57](#)

Description

The `threatfeedupdate` command is used to manually update the ETF engine.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example - Manually Updating External Threat Feeds Engine

In the following example, you can use the `threatfeedupdate` command to manually update the ETF engine.

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

Cluster Management

This section contains the following CLI commands:

clusterconfig

Description

The **clusterconfig** command is used to configure cluster-related settings. If this machine is not part of a cluster, running clusterconfig will give you the option of joining a cluster or creating a new cluster.

The **clusterconfig** command provides additional subcommands:

Non-Cluster Commands

The following commands are available when you are not in a cluster.

- **clusterconfig new <name>** — This will create a new cluster with the given name. This machine will be a member of this cluster and a member of a default cluster group called "Main Group".

<name> - The name of the new cluster.

- **clusterconfig join [--port=xx] <ip_of_remote_cluster> [<admin_password>]<groupname>** — This will add this machine to a cluster.

where:

<ip_of_remote_cluster> - The IP address of another machine in the cluster.

<admin_password > - The admin password of the cluster. This should not be specified if joining over CCS.

<groupname> - The name of the group to join.

<port> - The port of the remote machine to connect to (defaults to 22).

- **clusterconfig prepjoin print**

This will display the information needed to prepare the joining of this machine to a cluster over a CCS port.

Cluster Commands

The following commands are available when you are in a cluster.

- **clusterconfig addgroup <groupname>** — Creates a new cluster group. The group starts off with no members.
- **clusterconfig renamegroup <old_groupname> <new_groupname>** — Change the name of a cluster group.
- **clusterconfig deletegroup <groupname> [new_groupname]** — Remove a cluster group.

<groupname> - Name of the cluster group to remove.

<new_groupname> - The cluster group to put machines of the old group into.

- **clusterconfig setgroup <machinename> <groupname>** — Sets (or changes) which group a machine is a member of.

<machinename > - The name of the machine to set.

<groupname> - The group to set the machine to.

- **clusterconfig removemachine <machinename>** — Remove a machine from the cluster.

- `clusterconfig setname <name>` — Changes the name of the cluster to the given name.
- `clusterconfig list` — Display all the machines currently in the cluster.
- `clusterconfig connstatus` — Display all the machines currently in the cluster and add routing details for disconnected machines.
- `clusterconfig disconnect <machinename>` — This will temporarily detach a machine from the cluster.
 <machinename> - The name of the machine to disconnect.
- `clusterconfig reconnect <machinename>` - This will restore connections with machines that were detached with the “disconnect” command.
- `clusterconfig prepjoin new <serial_number> <hostname> <user_key>` — This will add a new host that is to join the cluster over the CCSport.
 <serial_number> - The serial number of the machine being added.
 <hostname> - The host name of the machine being added.
 <user_key> - The SSH user key from the "prepjoin print" command from the joining machine.
- `clusterconfig prepjoin delete <serial_number|hostname>` — This will remove a host that was previously indicated to be added from the "prepjoin new" command. This is only necessary to be used if you later decide not to add the host. When a host is successfully added to the cluster, its prepjoin information is automatically removed.

Usage

Commit: This command does not require a ‘commit’.

Cluster Management: This command is restricted to cluster mode.

Batch Command: This command does not support a batch format.

Example

For an explanation of the `clusterconfig` command and its uses, see *User Guide for AsyncOS for Cisco Secure Email Gateway* .

Data Loss Prevention

This section contains the following CLI commands:

dlpstatus

Request version information for DLP Engine.



Note DLP must already be configured via the DLP Global Settings page in the GUI before you can use the `dlpstatus` command.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is can be used at cluster, group or machine mode.

Batch Command: This command does not support a batch format.

Example

```
mail.example.com> dlpstatus

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

dlpupdate

Description

Update DLP Engine.



Note DLP must already be configured via the DLP Global Settings page in the GUI before you can use the **dlpupdate** command.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is can be used at cluster, group or machine mode.

Batch Command: This command supports a batch format.

Batch Format

The batch format of the dlpupdate command forces an update of the DLP engine even if no changes are detected.

```
dlpupdate [force]
```

Example

```
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.
[ ]>
```

Domain Exception List

This section contains the following CLI command:

domainrepconfig

Description

The `domainrepconfig` command is used to create a Domain Exception List.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: `help domainrepconfig`.

Example

In the following example, you can use the `domainrepconfig` command to create a Domain Exception List.

```
mail.example.com> domainrepconfig
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 Security Services

smimeconfig

Description

Configure S/MIME settings such as sending profiles, managing public keys, and so on.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Examples

Creating a Sending Profile for Signing and Encryption

The following example shows how to create a sending profile for signing and encrypting messages using S/MIME.

```
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.
[ ]>

```

Adding a Public Key for Encryption

The following example shows how to add the public key of the recipient's S/MIME certificate to the email gateway for encrypting messages.

```

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

```

Domain Keys

This section contains the following CLI commands:

domainkeysconfig

Description

Configure DomainKeys/DKIM support.

Usage

- Commit: This command requires a 'commit'.
- Cluster Management: This command can be used in all three machine modes (cluster, group, machine).
- Batch Command: This command supports a batch format.



Note For enhanced security, if encryption of sensitive data in the email gateway is enabled in FIPS mode, you will not be able view the private key. If you intend to edit the private key, you can enter an existing private key or generate a new private key.

Batch Format - Signing Profiles

The batch format of the domainkeysconfig command can be used to create, edit, or delete signing profiles

- Adding a DomainKeys/DKIM signing profile:

```

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

```

Table 1: domainkeysconfig New Signing Profile Arguments

Argument	Description
<name>	Name of domain profile.
<type>	Type of domain. Can be dk or dkim .
<domain>	Domain field of domain profile. This forms the d tag of the Domain-Keys signature.
<selector>	Selector field of domain profile. This forms the s tag of the Domain-Keys signature.

Argument	Description
<user-list>	Comma separated list of domain profile users. Users are used to match against email addresses to determine if a specific domain profile should be used to sign an email. Use the special keyword all to match all domain users.
[options]	
--key_name	The name of the private key that will be used for signing.
--canon	The canonicalization algorithm to use when signing by DK. Currently supported algorithms are simple and nofws . Default is nofws .
--body_canon	The body canonicalization algorithm of to use when signing by DKIM. Currently supported algorithms are simple and relaxed . Default is simple .
--header_canon	The headers canonicalization algorithm of to use when signing by DKIM. Currently supported algorithms are simple and relaxed . Default is simple .
--body_length	Number of bytes of canonicalized body that are used to calculate the signature. Is used only in DKIM profiles. If used this value becomes l tag of the signature. By default it is not used.
--headers_select	Detrmines how to select headers for signing. Is used only in DKIM profiles. Can be one of all , standard , standard_and_custom . all means to sign all non-repetitive headers. "standard" means to sign pedefined set of well known headers such as Subject, From, To, Sender, MIME heades etc. standard_and_custom means to sign well known headers and user-defined set of headers. Default is standard .
--custom_headers	User-defined set of headers to sign. Is used only in DKIM profiles if headers_select is standard_and_custom . Default is empty set.
--i_tag	Determines whether to include the i tag into the signature. Possible values are yes or no . Default is yes .
--agent_identity	The identity of the user or agent on behalf of which this message is signed. The syntax is a standard email address where the local-part may be omitted. Domain part of this address should be a sub-domain of or equal to the <domain> . This option is only applicable if --i_tag value is set to yes . Default is an empty local-part followed by an @ and by the <domain> .
--q_tag	Determines whether to include the q tag into the signature. Possible values are yes or no . Default is yes .
--t_tag	Determines whether to include the t tag into the signature. Possible values are yes or no . Default is yes .
--x_tag	Determines whether to include the x tag into the signature. Possible values are yes or no . Default is yes .
--expiration_time	Number of seconds before signature is expired. Is used only in DKIM profiles. This value becomes a difference of x and t tags of the signature. This option is only applicable if --x_tag value is set to yes . Default is 31536000 seconds (one year).

Argument	Description
--z_tag	Determines whether to include the z tag into the signature. Possible values are yes or no . Default is no .

- Editing a signing profile:

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

Signing profile options:

- 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
- Delete a signing profile:

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

- Show a list of signing profiles:

```
domainkeysconfig profiles signing list
```

- Print the details of a signing profile:

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

- Test a signing profile:

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

- Import a local copy of your signing profiles:


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

- Export a copy of your signing profile from the email gateway:

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

- Delete all the signing profiles from the email gateway:

```
domainkeysconfig profiles signing clear
```

Batch Format - Verification Profiles

- Create a new DKIM verification profile:

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

Table 2: domainkeysconfig Verification Profile Options

Argument	Description
--name	The name of DKIM verification profile.
--min_key_size	The smallest key to be accepted. Possible key-length values (in bits) are 512, 768, 1024, 1536 and 2048 . Default is 512 .
--max_key_size	The largest key to be accepted. Possible key-length values (in bits) are 512, 768, 1024, 1536 and 2048 . Default is 2048 .
--max_signatures_num	A maximum number of signatures in the message to verify. Possible value is any positive number. Default is 5 .
--key_query_timeout	A number of seconds before the key query is timed out. Possible value is any positive number. Default is 10 .
--max_systemtime_divergence	A number of seconds to tolerate wall clock asynchronization between sender and verifier. Possible value is any positive number. Default is 60.
--use_body_length	Whether to use a body length parameter. Possible values are yes or no . Default is yes .
--tempfail_action	The SMTP action should be taken in case of temporary failure. Possible values are accept or reject . Default is accept .
--tempfail_response_code	The SMTP response code for rejected message in case of temporary failure. Possible value is number in 4XX format. Default is 451 .
--tempfail_response_text	The SMTP response text for rejected message in case of temporary failure. Default is #4.7.5 Unable to verify signature - key server unavailable .

Argument	Description
--permfail_action	The SMTP action should be taken in case of permanent failure. Possible values are accept or reject . Default is accept .
--permfail_response_code	The SMTP response code for rejected message in case of permanent failure. Possible value is number in 5XX format. Default is 550 .
--permfail_response_text	The SMTP response text for rejected message in case of permanent failure. Default is #5.7.5 DKIM unauthenticated mail is prohibited.

- Edit a verification profile:

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

- Delete a verification profile:

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

- Print details of an existing verification profile:

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

- Display a list of existing verification profiles:

```
domainkeysconfig profiles verification list
```

- Import a file of verification profiles from a local machine:

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

- Export the verification profiles from the email gateway:

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

- Delete all existing verification profiles from the email gateway:

```
domainkeysconfig profiles verification clear
```

Batch Format - Signing Keys

- Create a new signing key:

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

Table 3: domainkeysconfig Signing Keys Options

Argument	Description
--generate_key	Generate a private key. Possible key-length values (in bits) are 512 , 768 , 1024 , 1536 , and 2048 .
--use_key	Use supplied private key.
--public_key	Flag to derive and print to the screen a matching public key for the specified private key. If --generate_key is specified first, a new private key is generated first, followed by the display of a matching public key.

- Edit a signing key:

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

- Rename an existing signing key:

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

- To specify a public key:

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

- Delete a key:

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

- Display a list of all signing keys:

```
domainkeysconfig keys list
```

- Display all information about a specify signing key:

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

- Import signing keys from a local machine:

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

- Export signing keys from the email gateway:

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

- Delete all signing keys on the email gateway:

```
domainkeysconfig keys clear
```

Batch Format - Search for a Key or Profile

- Search for a profile signing key:

```
domainkeysconfig search <search_text>
```

Batch Format - Global Settings

- Modify global settings for Domain Keys/DKIM on your email gateway:

```
domainkeysconfig setup <setup_options>
```

The option available is:

- `--sign_generated_msgs` - Specify whether to sign system-generated messages. Possible values are yes or no .

Example: Configuring Domain Keys via the CLI

Use the `domainkeysconfig` command in the CLI to configure Domain Keys on your email gateway.

The `domainkeysconfig` command has all of the features of the **Mail Policies -> Domain Keys** page. It also provides the ability to generate a sample Domain Keys DNS TXT record. For more information about generating sample Domain Keys DNS TXT records, see [Creating a Sample Domain Keys DNS TXT Record, on page 73](#).

In this example, a key is generated, and a domain profile is created:

```
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
```

Example: Configuring Domain Keys via the CLI

```

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:
[1]> 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.
[1]>
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[1]>
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.
[]>
```

Creating a Sample Domain Keys DNS TXT Record

```
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
1f0Op1AzSuE2BvOrxZ5Nr+se0T+k7mYDF0FSUHywAoV+kCum7fFRjS3E0F9gIpbIdH5vzCKp/w7hdjPy3q6PsgJVtqvQ6v9E8k5ui7C+DF6KwJUiMJSY5sbu2
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 Verification

This section contains the following CLI commands:

dmarcconfig

Description

Configure DMARC settings.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format - DMARC Verification Profiles

The batch format of the dmarcconfig can be used to create, edit, or delete verification profiles and modify global settings.

Add a DMARC Verification Profile

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

Argument	Description
<name>	Name of the DMARC profile.
[options]	
--rejectpolicy_action	The message action that AsyncOS must take when the policy in DMARC record is reject. Possible values are "reject", "quarantine", or "none."

Argument	Description
--rejectpolicy_response_code	The SMTP response code for rejected messages. The default value is 550.
--rejectpolicy_response_text	The SMTP response text for rejected messages. The default value is “#5.7.1 DMARC unauthenticated mail is prohibited.”
--rejectpolicy_quarantine	The quarantine for messages that fail DMARC verification.
--quarantinepolicy_action	The message action that AsyncOS must take when the policy in DMARC record is quarantine. Possible values are “quarantine” or “none.”
--quarantinepolicy_quarantine	The quarantine for messages that fail DMARC verification.
--tempfail_action	The message action that AsyncOS must take on the messages that result in temporary failure during DMARC verification. Possible values are “accept” or “reject.”
--tempfail_response_code	The SMTP response code for rejected messages in case of temporary failure. The default value is 451.
--tempfail_response_text	The SMTP response text for rejected messages in case of temporary failure. The default value is “#4.7.1 Unable to perform DMARC verification.”
--permfail_action	The message action that AsyncOS must take on the messages that result in permanent failure during DMARC verification. Possible values are “accept” or “reject.”
--permfail_response_code	The SMTP response code for rejected messages in case of permanent failure. The default value is 550.
--permfail_response_text	The SMTP response text for rejected messages in case of permanent failure. The default value is “#5.7.1 DMARC verification failed.”

Edit a DMARC Verification Profile

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

Delete a DMARC Verification Profile

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

Delete all the DMARC Verification Profiles

```
dmarcconfig profiles clear
```

View the Details of a DMARC Verification Profile

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

Export DMARC Verification Profiles

```
dmARCconfig profiles export <filename>
```

Import DMARC Verification Profiles

```
dmARCconfig profiles import <filename>
```

Change Global Settings

```
dmARCconfig setup [options]
```

Options	Description
--report_schedule	The time when you want AsyncOS to generate DMARC aggregate reports.
--error_reports	Send delivery error reports to the domain owners if the DMARC aggregate report size exceeds 10 MB or the size specified in the RUA tag of DMARC record.
--org_name	The entity generating DMARC aggregate reports. This must be a domain name.
--contact_info	Additional contact information, for example, details of your organization's customer support, if the domain owners who receive DMARC aggregate reports want to contact the entity that generated the report.
--copy_reports	Send copy of all the DMARC aggregate reports to specific users, for example, internal users who perform analysis on the aggregate reports. Enter an email address or multiple addresses separated by commas.
--bypass_addresslist	Skip DMARC verification of messages from specific senders (address list). Note You can choose only address lists created with full email addresses.
--bypass_headers	Skip DMARC verification of messages that contain specific header field names. For example, use this option to skip DMARC verification of messages from mailing lists and trusted forwarders. Enter a header or multiple headers separated by commas.

Example

The following example shows how to setup a DMARC verification profile and edit the global settings of DMARC verification profiles.

```
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

This section contains the following CLI commands:

dig

Description

Look up a record on a DNS server

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

The batch format of the dig command can be used to perform all the functions of the traditional CLI command.

- Look up a record on a DNS server

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

- Do a reverse lookup for given IP address on a DNS server

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

These are the options available for the dig command's batch format

-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.

Example

The following example explicitly specifies a DNS server for the lookup.

```
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
```



Note The **dig** command filters out the information in the Authority and Additional sections if you do not explicitly specify the DNS server when using the command.

Example: Verifying TLSA Record of the DNS Server Supporting DNSSEC

The following example explicitly verifies TLSA records.

```
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+t0W9a0qDMvxytXfkrms+IEUbK1Ct9XB5mBCCb3bHryvHs0cU6XPxTJ
XwQ5HUSWuQaC9MLyCA5Zn/AX1bzKA7tGtnab0q3CmVKhhRXnIJ+jJht6
nuksUrLksM6uYmR73DDM/bCC8n08w6nGeGq476mmNgETXAPfqSvHNuPp
DSquCG3nNfm8iE9XnG8jCKRPcKhWjROc/vmK6ZzuzFKctT4QA/L5Ah0w
zffZqxR9Qmj3w8WQdz9eFAw5e0Lfa5oR57i983ityJrQL4pjF17bwKNw
94xhqFlsWWKAC6wpoT64DOo00ou5TsKxHq5EwEat1OMIM0GHMniCuJcA K3seyQ==

```

dnsconfig

Description

Configure DNS setup

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

The batch format of the dnsconfig command can be used to perform all the functions of the traditional CLI command.

- Configuring DNS to use a local nameserver cache:

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

Command arguments:

- <ns_ip> - The IP address of the nameserver. Separate multiple IP addresses with commas.
- <priority> - The priority for this entry.
- Deleting the local nameserver cache:

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

- Configuring alternate DNS caches to use for specific domains:

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



Note Cannot be used when using Internet root nameservers.

Command arguments:

- <ns_ip> - The IP address of the nameserver. Separate multiple IP addresses with commas.
- <domains> - A comma separated list of domains.
- Deleting the alternate DNS cache for a specific domain:

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

- Configuring DNS to use the Internet root nameservers:

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

Nameserver arguments:

- <ns_domain> - The domain to override.
- <ns_name> - The name of the nameserver.
- <ns_ip> - The IP address of the nameserver.



Note You can override certain domains by specifying an alternate name server for that domain.

- Deleting nameservers:

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



Note When deleting, if you do not specify an ns_name , then all nameservers for that domain will be removed.

- Clearing all DNS settings and automatically configuring the system to use the Internet root servers:

```
dnsconfig roots
```

Displaying the current DNS settings.

```
dnsconfig print
```


Example

Each user-specified DNS server requires the following information:

- Hostname
- IP address
- Domain authoritative for (alternate servers only)

Four subcommands are available within the **dnsconfig** command:

Table 4: Subcommands for dnsconfig Command

Syntax	Description
new	Add a new alternate DNS server to use for specific domains or local DNS server.
delete	Remove an alternate server or local DNS server.
edit	Modify an alternate server or local DNS server.
setup	Switch between Internet root DNS servers or local DNS servers.

```
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]> 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.
[ ]>
```

Adding an Alternate DNS Server for Specific Domains

You can configure the email gateway to use the Internet root servers for all DNS queries except specific local domains.

```
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.
[]>
```

Using Your Own DNS Cache Servers

You can configure the email gateway to use your own DNS cache server.

```
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

Description

Clear all entries from the DNS cache.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

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

dnshostprefs

Description

Configure IPv4/IPv6 DNS preferences

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```
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.
[1]> 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.
[1]>

```

dnslistconfig

Description

Configure DNS List services support

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```

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.
[1]> 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.
[1]>

```

dnslsttest

Description

Test a DNS lookup for a DNS-based list service.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```
mail3.example.com> dnslsttest
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

Description

Display DNS statistics.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
mail3.example.com> dnsstatus
Status as of: Mon Apr 18 10:58:07 2005 PDT
Counters:
DNS Requests          Reset      Uptime      Lifetime
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
```

Enhanced User Experience using How-Tos Widget

This section contains the following CLI commands:

howtoupdate

Description

The `howtoupdate` command is used to manually update the How-Tos component.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: `help howtoupdate`.

Example

In the following example, you can use the `howtoupdate` command to manually update the How-Tos component.

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

howtostatus

Description

The `howtostatus` command is used to display the current version of the How-Tos component.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: `help howtostatus`.

Example

In the following example, you can use the `howtostatus` command to view the current version of the How-Tos component.

```
mail.example.com > howtostatus

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

General Management/Administration/Troubleshooting

This section contains the following CLI commands:

addressconfig

Description

The **addressconfig** command is used to configure the From: Address header. You can specify the display, user, and domain names of the From: address. You can also choose to use the Virtual Gateway domain for the domain name. Use the **addressconfig** command for mail generated by AsyncOS for the following circumstances:

- Anti-virus notifications
- Bounces
- DMARC feedback reports
- Notifications (`notify()` and `notify-copy()` filter actions)
- Quarantine Messages (and “Send Copy” in quarantine management)
- Reports
- All other messages

In the following example, the From: Address for notifications is changed from: Mail Delivery System [MAILER-DAEMON@domain] (the default) to Notifications [Notification@example.com]

Usage

Commit: This command requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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

Description

Use the **adminaccessconfig** command to configure:

- Login message (banner) for the administrator.
- IP-based access for email gateway administrative interface.
- Web interface Cross-Site Request Forgeries protection.
- Option to use host header in HTTP requests.
- Web interface and CLI session inactivity timeout.
- Maximum HTTP header size.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

The batch format of the **adminaccessconfig** command can be used to perform all the functions of the traditional CLI command.

- Select whether to allow access for all IP addresses or limit access to specific IP address/subnet/range

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

- Adding a new IP address/subnet/range

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

- Editing an existing IP address/subnet/range


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

- Deleting an existing IP address/subnet/range

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

- Printing a list of the IP addresses/subnets/ranges

```
adminaccessconfig ipaccess print
```

- Deleting all existing IP addresses/subnets/ranges

```
adminaccessconfig ipaccess clear
```

- Printing the login banner

```
adminaccessconfig banner print
```

- Importing a login banner from a file on the email gateway

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

- Deleting an existing login banner

```
adminaccessconfig banner clear
```

- Printing the welcome banner

```
adminaccessconfig welcome print
```

- Importing a welcome banner from a file on the email gateway

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

- Deleting an existing welcome banner

```
adminaccessconfig welcome clear
```

- Exporting a welcome banner

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

- Add an allowed proxy IP address

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

- Edit an allowed proxy IP address

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

- Delete an allowed proxy IP address

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

- Delete all existing allowed proxy IP addresses

```
adminaccessconfig ipaccess proxylist clear
```

- Configure the header name that contains origin IP address

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

- Enable or disable web interface Cross-Site Request Forgeries protection

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

- Check whether web interface Cross-Site Request Forgeries protection is enabled

```
adminaccessconfig csrf print
```

- Configure web interface session timeout

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

- Configure CLI session timeout

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

Example - Configuring Network Access List

You can control from which IP addresses users access the email gateway. Users can access the email gateway from any machine with an IP address from the access list you define. When creating the network access list, you can specify IP addresses, subnets, or CIDR addresses.

AsyncOS displays a warning if you do not include the IP address of your current machine in the network access list. If your current machine's IP address is not in the list, it will not be able to access the email gateway after you commit your changes.

In the following example, network access to the email gateway is restricted to two sets of IP addresses:

```
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.
- XSS - Configure Cross-Site Scripting Attack protection.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSize - Configure maximum HTTP header field size.
- HOW-TOS - Configure How-Tos feature.
[]> 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.
[]>

```

Example - Configuring Login Banner

You can configure the email gateway to display a message called a “login banner” when a user attempts to log into the email gateway through SSH, Telnet, FTP, or Web UI. The login banner is customizable text that appears above the login prompt in the CLI and to the right of the login prompt in the GUI. You can use the login banner to display internal security information or best practice instructions for the email gateway. For example, you can create a simple note that saying that unauthorized use of the email gateway is prohibited or a detailed warning concerning the organization’s right to review changes made by the user to the email gateway.

Example - Configuring Web Interface and CLI Session Timeout

The maximum length of the login banner is 2000 characters to fit 80x25 consoles. A login banner can be imported from a file in the /data/pub/configuration directory on the email gateway. After creating the banner, commit your changes.

In the following example, the login banner “Use of this system in an unauthorized manner is prohibited” is added to the email gateway:

```
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.
- XSS - Configure Cross-Site Scripting Attack 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.
- HOW-TOS - Configure How-Tos feature.
[]> 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.
[]>
```

Example - Configuring Web Interface and CLI Session Timeout

The following example sets the web interface and CLI session timeout to 32 minutes.



Note The CLI session timeout applies only to the connections using Secure Shell (SSH), SCP, and direct serial connection. Any uncommitted configuration changes at the time of CLI session timeout will be lost. Make sure that you commit the configuration changes as soon as they are made.

```
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.
- XSS - Configure Cross-Site Scripting Attack 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.
- HOW-TOS - Configure How-Tos feature.

[]> 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

```



Note After committing the changes, the new CLI session timeout takes affect only during the subsequent login.

certconfig

Description

Configure security certificates and keys.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example - Pasting in a certificate

In the following example, a certificate is installed by pasting in the certificate and private key.

```

mail1.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

```

Example - Pasting in a certificate

```

Name          Common Name          Issued By          Status          Remaining          FQDN
Compliance checked
-----
Demo          Cisco Appliance Demo  Cisco Appliance Demo  Active          3467 days          No
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-----
MIICLDCCAyCAQAwDQYJKoZIhvcNAQEEBQAwwgAxCzAJBgNVBAYTAlBUMRMwEQYD
VQQUeWpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNlb2ExFzAVBgNVBAoTDk5ldXJv
bmlvLlCBMzZGEuMRgwFgYDVQQLEw9EZXN1bnZvbHJpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCsGSIb3DQEJARYMc2FtcG9AaWtpLmZpMjB4X
DTk2MDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2NDk2
EQYDVQQIEWpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNlb2ExFzAVBgNVBAoTDk5ldXJv
bmlvLlCBMzZGEuMRgwFgYDVQQLEw9EZXN1bnZvbHJpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCsGSIb3DQEJARYMc2FtcG9AaWtpLmZpMjB4X
MFwwDQYJKoZIhvcNAQEEBQAQSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTdlkjNw
L41YKbpzzlmC5beaQXeq2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAATAN
BgkqhkiG9w0BAQQFAANBAFqPEKfjk6T6CKTHvaQeEAsX0/8YHPHqH/9AnhSjrwuX
9EBc0n6bVGHn7XaXd6sJ7dym9sbsWxb+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/+yxjxv4q1MUTdlkjNwL41YKbpzzlmC5beaQXeq
2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAAQJBALjkK+jc2+iihI98riEF
oudmknZiSRTYjnwjx8mCoAjPWviB3c742e03FG4/soiljd9A5alihEOXfUzloenr
8IECIQD3B5+0l+68BA/6d76iUNqAAV8djGTzvxncXycncxPQydQIhAMxt4trUI3nc
a+U8YL2HPPFA3gmhBsSICbq2OptOCnM7hAIEA6Xi3JIQECob8Ywkrj29DU3/4WYD7
WLPgsQpwolGuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IZmxcLpRcpslpeWBBaIEA
6/5B8J0GHDJq89FHwEG/H2eVVUYu5y/ad6sgcm+0Avg=
-----END RSA PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n

Do you want to check if Common Name is in Fully Qualified Domain Name (FQDN) format ? [N]>
yes

List of Certificates
Name          Common Name          Issued By          Status          Remaining          FQDN
Compliance Checked
-----
partner.c brutus.partner.com brutus.partner      Active          30 days          Yes
 Demo          Cisco Appliance Demo  Cisco Appliance Demo  Active          3467 days          No
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

```

Example - Creating a Self-signed Certificate

In the following example, a self-signed certificate is created.

```

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
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN)
format ? [N]>
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

```

Example - Create a Self-signed S/MIME Signing Certificate

```

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDELMAkGALUEBhMCVVMxFDASBgNVBAMTC2V4YW1wbGUuY29t
MRYwFAYDVQQHEW1TYW4gRnJhbmNpc29jMRAwDgYDVQQKEWdleGFtcGx1MQswCQYD
VQQIEwJkQTEEMMAoGAlUECXMdb3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEANwamZyX7VgTZka/xlI5HHRN9V2MPKXoLq7FjzUtiIDwznElrKIuJovw
Svonle6GvFlUHfjv8B3WobOzk5Ny6btKjwPrBfaY+qr7rzM4lAQKHM+P6l+lZnPU
P05N9RCkLP4XsUuyY6Ca1WLTiPIgaq2fR8Y0JX/kesZcGOqlde66pN+xJIHHYadD
oopOgqi6SLNFazJu/HEu/fnSujG4nhF0ZGLOpVUx4fg33NwZ4wV10XBk3GrOjbbA
ih9ozAwfNzxb57amtxEJk+pW+co3uEHLJIOPdih9SHzn/UUV4hiu8rSQR19sDApp
kfdWcfaDLF9tnQJPWSYoCh0USgCc8QIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEB
AGiVhyMAZuHsv9yA08kJCmrgO89yRlnDUXDDo6IrODVKx4hHTiOanOPulnsThSvH
7xV4xR35T/QV0U3yPrL6bJbbwMySOLIRTjsUcwZnjOE1xMM5EkBM2BOI5rs4l59g
FHhVejhG1LyyUDL0U82wsSLMqLFH1IT63tzwVmRiIXmAu/lHYci3+vctb+sopnN1
lY1OIuj+EggWnrRBNnKXLTdXkzhELOd8vZEgSAfBWYjZ2mECzC7SG3evqkw/OGLk
AilNXHayiGjeY+UfWzF/HBSekSJtQu6hIv6JpBSY/MnYU4tllExqD+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
[]>

```

Example - Create a Self-signed S/MIME Signing Certificate

The following example shows how to create a self-signed S/MIME certificate for signing messages.

```

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
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN)
format ? [N]>

```



```

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
[]>

```

date

Description

Displays the current date and time

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

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

```

daneverify

- [Description, on page 100](#)
- [Usage, on page 100](#)
- [Example, on page 100](#)

Description

Checks whether DANE is supported for a specified domain.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: `help daneverify`.

Example

In the following example, you can use the `daneverify` command to verify DANE support for a specified domain.

```
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_SUCESS for example-dane.net
DANE verification completed.
```

diagnostic

Description

Use the diagnostic command to:

- Troubleshoot hardware and network issues using various utilities
- Check the RAID status
- Display ARP cache
- Clear LDAP, DNS, and ARP caches
- Send SMTP test messages
- Restart and viewing the status of Service Engines enabled on the email gateway.

Using the diagnostic Command

The following commands are available within the diagnostic submenu:

Table 5: diagnostic Subcommands

Option	Sub Commands	Availability
RAID	1. Run disk verify	Available on C30 and C60 only.
	2. Monitor tasks in progress	
	3. Display disk verify verdict	
DISK_USAGE (deprecated)	No Sub Commands	This command has been deprecated. Instead, use the diskquotaconfig command.
NETWORK	FLUSH	C- and M-Series
	ARPSHOW	
	SMTTPING	
	TCPDUMP	
REPORTING	DELETEDB	C- and M-Series
	DISABLE	
TRACKING	DELETEDB	C- and M-Series
	DEBUG	
RELOAD	No Sub Commands	C- and M-Series
SERVICES	RESTART	C- and M-Series
	STATUS	

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command supports a batch format.

Batch Format

The batch format of the diagnostic command can be used to check RAID status, clear caches and show the contents of the ARP cache. To invoke as a batch command, use the following formats:

Use the batch format to perform the following operations:

- Check the RAID status

```
diagnostic raid
```

- Show the contents of the ARP cache

```
diagnostic network arpshow
```

- Show the contents of the NDP cache

```
diagnostic network ndpshow
```

- Clear the LDAP, DNS, ARP and NDP caches

```
diagnostic network flush
```

- Reset and delete the reporting database

```
diagnostic reporting deletedb
```

- Enable reporting daemons

```
diagnostic reporting enable
```

- Disable reporting daemons

```
diagnostic reporting disable
```

- Reset and delete the tracking database

```
diagnostic tracking deletedb
```

- Reset configuration to the initial manufacturer values

```
diagnostic reload
```

Example: Displaying and Clearing Caches

The following example shows the **diagnostic** command used to display the contents of the ARP cache and to flush all network related caches.

```
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.
- 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.

```

Example: Verify Connectivity to Another Mail Server

The following example shows diagnostics used to check connectivity to another mail server. You can test the mail server by sending a message or pinging the server.

```

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.

```

Example: Reset Email Gateway Configuration to the Initial Manufacturer Values

```

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.

```

Example: Reset Email Gateway Configuration to the Initial Manufacturer Values

The following example shows how to reset your email gateway configuration to the initial manufacturer values.

```

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

```

Restarting and Viewing Status of Service Engines

You can use the `diagnostic > servicessub` command in the CLI to:

- Restart the service engines enabled on your email gateway without having to reboot your email gateway.
- View the status of service engines enabled on your email gateway.

For more information, refer to the CLI Reference Guide for Cisco Secure Email Gateway.

diskquotaconfig

View or configure disk space allocation for reporting and tracking, quarantines, log files, packet captures, and configuration files.

See *User Guide for AsyncOS for Cisco Secure Email Gateway* for complete information about this feature.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

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

Valid values for <feature> are euq , pvo , tracking , reporting

Valid values for <quota> are integers.

Example

```
mail.example.com> diskquotaconfig
Service                                     Disk Usage(GB)   Quota(GB)
-----
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                                     Disk Usage(GB)   Quota(GB)
-----
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

Set or clear the enrollment client that is used to obtain certificates for use with the URL Filtering feature.

Do not use this command without guidance from Cisco support.

Entries must be in the format <hostname:port> or <IPv4 address:port> . Port is optional.

To specify the default server, enter ecconfig server default .

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used at all levels in a cluster.

Batch Command: This command supports a batch format.

Batch Format

- To specify a non-default enrollment client server:

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

To use the default enrollment client server:

```
> ecconfig server default
```

Example

```
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

Display the current version of the enrollment client that is used to automatically obtain certificates for use with the URL Filtering feature.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

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


ecupdate

Manually update the enrollment client that is used to automatically obtain certificates for use with the URL Filtering feature. Normally, these updates occur automatically. Do not use this command without guidance from Cisco support.

If you use the force parameter (ecupdate [force]) the client is updated even if no changes are detected.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

```
> ecupdate [force]
```

Example

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

encryptionconfig

Configure email encryption.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

The following example shows modifications to an encryption profile:

```
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.)
```

Example

```
[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: AES-192
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
- APPLET - 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: AES-192
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: AES-192
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
- APPLET - 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

Description

The **encryptionstatus** command shows the version of the PXE Engine and Domain Mappings file on the email gateway, as well as the date and time the components were last updated.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```

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

Description

The **encryptionupdate** command requests an update to the PXE Engine on the email gateway.

Usage

Commit: This command does not require a ‘commit’.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command does not support a batch format.

Example

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

enginestatus

Description

The **enginestatus** command is used to display the status and CPU usage of various engines enabled on the email gateway.

Usage

Commit: This command does not requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: help enginestatus.

Example

The following example shows how to view the status and CPU usage of all engines enabled on the email gateway:

```
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          01-392.68             N10 Nov 2016 07:08 (GMT
+00:00) updated
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

Description

The **featurekey** command lists all functionality enabled by keys on the system and information related to the keys. It also allows you to activate features using a key or check for new feature keys.

For virtual email gateways, see also [loadlicense, on page 347](#) and [showlicense , on page 348](#).

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

In this example, the **featurekey** command is used to check for new feature keys.

```

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

Description

The **featurekeyconfig** command allows you to configure the machine to automatically download available keys and update the keys on the machine.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In this example, the featurekeyconfig command is used to enable the autoactivate and autocheck features.

```
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

Description

The **generalconfig** command allows you to configure browser settings.

Usage

Commit: This command requires 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For details, see the inline help by typing the command: help generalconfig .

Example - Configure Internet Explorer Compatibility Mode Override

The following example shows how to override IE Compatibility Mode.

```
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

Description

Checks the health of your email gateway. Health check analyzes historical data (up to three months) in the current Status Logs to determine the health of the email gateway.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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 page swapping
High memory usage

For more information about these problems and how to remediate them, see the TechNote
http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html
```

healthconfig

Description

Configure the threshold of various health parameters of your email gateway such as CPU usage, maximum messages in work queue and so on

Usage

Commit: This command requires 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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

Description

The **ntpconfig** command configures AsyncOS to use Network Time Protocol (NTP) to synchronize the system clock with other computers. NTP can be turned off using the **settime** command.

Usage

Commit: This command requires 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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

The Cisco Talos Email Status Portal is a web-based tool for monitoring the status of email submissions from end-users. This portal requires all your email gateways to have a common registration ID.

Use the **portalregistrationconfig** command in CLI to set the registration ID. If your email gateways are not part of a cluster, you must set a common registration ID on all your email gateways.

For more information about the portal, see Managing Spam and Graymail chapter in user guide or online help.

Usage

Commit: This command requires 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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

Description

Restart the email gateway.

Usage

Commit: This command does not require a 'commit'.

Example

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Request version information of Reputation Engine.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Resume receiving and deliveries

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
mail3.example.com> resume
Receiving resumed for Listener 1.
```

```
Mail delivery resumed.  
Mail delivery for individually suspended domains must be resumed individually.
```

resumedel

Description

Resume deliveries.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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.
```

resumelister

Description

Resume receiving on a listener.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

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

revert

Description

Revert to a previous release.

Usage

Commit: This command does not require a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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]>
```

samlconfig

- [Description, on page 120](#)
- [Usage, on page 121](#)
- [Example – Configure New SAML Profile, on page 121](#)
- [Example – Modifying SAML Profile, on page 123](#)

Description

Configure SAML profile with Service Provider and Identity Provider Settings.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, and machine).

Batch Command: This command does not support a batch format.

Example – Configure New SAML Profile

In the following example, the `samlconfig` command is used to create a new SAML Profile with service provider and identity provider settings. You must enter a valid certificate and the private key for the service provider. You can either configure the identity provider configuration manually or import an existing identity provider metadata.

```
mail.example.com > samlconfig
Choose the operation you want to perform:
- UILOGIN - Create a new SAML Profile for UI Login.
[]> uillogin
No SAML profiles are configured on the system.
Choose the operation you want to perform:
- NEW - Create a new SAML profile.
[]> new
Please enter the Service Provider Settings:
Enter the SP profile Name:
[]> SP1
Enter the SP Entity Id:
[]> ENTSP
Name ID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer URL: http://mail.example.com
Please paste the SP Certificate
.
Paste the content now.
Press CTRL-D on a blank line when done.
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmGAWIBAgIJAPSTH66oUo0kMA0GCSqGSIb3DQEBBQUAMC8xLTAarBNV
BAMMJHZtMjFlc2EwMTMzLmNzZmJlZGV2aXQuY2l2Y29sYWJzLmNvbTAeFw0xOTA1
MDkxMzA3NDRaFw0yOTA1MDYxMzA3NDRaMC8xLTAarBgNVBAMMJHZtMjFlc2EwMTMz
LmNzZmJlZGV2aXQuY2l2Y29sYWJzLmNvbTCCASIdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAM1/iDEkYMKOXXU+XWQr+KrDxdNxq3tCkqLmZwFH4TjzYLIwKsX
BZt8mlGiiEn/8ilBHlNDtju399qi7ZdSV2OIozrIqm9tPsgGCfoi90F3AM0WYTP
BWxi6MaJMjPlIka01ZvVLvqXjUcSM2esAsLNY1qMZ/MDqK/x11FWK5qCh/2J9n9n
4NuRpXsZDqCq4ERKhHOizr01esoqKEF3Cn9yDDkFQb4NgRC9CDNWCIF7jbdIcd5T
H4nIus2k5dyo57NIZtdLhLFidUFJ0MycGXZfo7+AHuST0ofnTxgz1o3ZpcxwZl4m
40UNOQhK7DrBdfSAAjITpyAZ1CuXIKnLkEsCAwEAAANQME4wHQYDVR0OBBYEFKWK
siiXt1Qfe/EXFhEnTuZoJzoCMB8GA1UdIwQYMBaAFKWKsiiXt1Qfe/EXFhEnTuZo
JzoCMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBADuzDA0iqITrrZC/
jEdwlbz5rbJCMu96mDLh2zzjvQj5K8WNBkTa/UDcj42+2fP+w+DfIjeKcZwUTHGp
TMmVsLAtuL8oF2uKuNhGUD8tVvqbRFAgb7OefOfYWXKjDyhfNsWxohNemDne+RZC
DZ7bS/NG2Wkj0wiZBUCj42+0emtDDa0k2Imi/LquZnQomNfsid2OZiAh89gfEgRU
zogadeWGTGTOb2bDlU4pwaLx+4gKI25ZjpFtk6ak4p8NDZGNDZE3r4IvsP9mlSse
0IA+RwGBbgQxnFuuh9s8Nux1DzNj38Pb6qedjujwIHh3TTYETU3rS5jBwnlJdsmt
2po7pB8=
-----END CERTIFICATE-----
Please paste the SP Certificate Key
.
Paste the content now.
Press CTRL-D on a blank line when done.
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAzX+IMSRgwo5ddT5dZCv4qsPF03Gre0KSouZnAUFhOPPFgja
qxcFm3yaUaKKUSf/yKUEeU00207f32qLtl1JXY4ijOsiqb20+yAYJ+iL3QXcAzRZ
hm8FZeLoxokwk+UiQDSVm9UtWpeNRxIzZ6wCws1jWqbP8wOor/HXUVYrmoKH/Yn2
f2fg25GLexkOoKrgREqEc6L0s7V6yiooQXcKf3IMOQVBvg2BEL0IM1YIgxUnT0hw
```

Example – Configure New SAML Profile

```

P1Mfici6zaTl3Kjns0hm10uEsWJlQUnQzJwZdl87v4Ae5JFSh+dPGDPWjdmlzHBm
XibjRQ05CErsOsEN9IACMhOnIBnUK5cgqcuQSwIDAQABAoIBAGkPxK9rK9UMObfT
FKg8GtwjTyalPLi95n5GUW9EMO+NgfNfc8uE76b442TNNu4bBxir1Ue279pU9jwh
GuDXfMTKADwPxx85ECg7l13A9JDBiCRTRVzkzBk163wtx5FYYl2RBziNnr9JbHS2y
zkn4Zgj2PM+B7VsPCdU6T20V8yEAo75PtmZfmwq/Z1zMmIhDiFJqXZuxH7vYCP+y
3ZeBpP09Y0u4Rz8x9MpUPG8z+b9ekoLd8K90YQqdTZPqaG3MD8SEeKLSYlByOk1B
mGZWvVRRfEnjEPsjixxiLsdD8RFL+18SazI5Zfmr1GM1lMcUcQ4zz8Wds5I2Zi
FhqW7vECgYEA+76Af/U7joUApXjzrm7MfLHO/w+OKrPJJdCl3V5PZtGgmJTkrf33
7+kv3zlnyObf5myErFlCtFYqJ3QA/taolK1PdE4EFpIJevxA7PF2hH0Ee51YCx5v
T8G/dSOFSDm+3oaXr3WQZfNPBOWBxltb+0EaHG553HtQQGAfTe1l2UCgYEA0Pjj
AtE2t5IwV2xehBU7X1DkUSFITz6nHlkB/4jehQWbT3pulBctBfGeEfPMxrenMolt
kcNQ3pw6vo4ZeHrxG6A3KYWqPVnlhXOYo7z1evbUGWnAQrSb9eCEZy1910oXW16F
E5X2WQ/ENz8YDa/XqOJ6IivW++dsBfhEAzRRe8CgYAktfodLTDzjrGyrGPUuxmc
OX0jGsybk44wsoWNi5Q+pTErLwNOECwY000E50UqmPXDLD24FiBq/G5WYHUWL5Be/
Xqqohjv4YqF5StHY+7lRxlhWdab7zBv7pAxcZI6wrXfn8eOiGtjFaomyNanrYC
JNM+8y1b//QeN67LJfe4NQKBgBcURc4b2RUxGhGtsEqaJbJm8LBdIqVN4BsJ7WqR
bTH3yo1ekjPc02YipziWodf4k28+9LrZVUQoBRHkVyTB2nrqev2DTU1Znn0qFj9
F4d7FzWvTkKpu+HN6BGVhp6TM/0tVTkyiMCRUzRezYNFdmX6jU5m411zv0UlDgA9
yicVAoGBAJHY4jbd9mi+u87ss6yT4ETHmzauxd14ohEQmNm9YqBeaNC1LRrzQoM
JhK1xSx55X21r+2Iizg6DVJ3GFpc+Kfwp86676J08tWfad+3mnHtRqSSFEaV/7Ik
Yf09kYdhDAVLU4BFmBQ5Fi8Brx6Bmi2MpjTP1CsTStAkAnB2KZuV
-----END RSA PRIVATE KEY-----
^Enter the SP Certificate Passphrase:
[]>
Do you want to Sign Requests:
[]>
Do you want to Sign Assertion Requests:
[]>
Enter the Technical Contact Id:
[]> mail@example.com
Enter the Organization URL:
[]> http://www.example.com
Enter the Organization Name:
[]> Example
Enter the Organization Display Name:
[]> Example
Please enter the Identity Provider Settings:
Enter the IDP Profile Name:
[]> IDP1
Choose the operation you want to perform:
- PASTE - Paste the IDP Metadata XML.
- ENTER - Enter the IDP Metadata
[]> paste
Please paste the IDP Metadata XML
.
Paste the content now.
Press CTRL-D on a blank line when done.
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  entityID="https://WIN-BL0P4116VDB/dag/saml2/idp/metadata.php">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDYTCCAkmGAWIBAgIBAAANBgkqhkiG9w0BAQsFADBLMQ
swCQYDVQQGEwJVUzELMAkGA1UECAwCTUkxEjAQBgNVBAcMCUFubiBBcmJvcjEbmBkG
AlUECgwSRHVvIFNlY3VyaXR5LzBjbmMuB4XDTE5MDQyOTeWMTQxMFoXDTI5MDQyNjE
wMTQxMFoXDTI5MDQyNjEwMTQxMFoXDTI5MDQyNjEwMTQxMFoXDTI5MDQyNjEwMTQx
b3IxGzAZBgNVBAoMEkRlbyBTZW51cml0eSwgSW5lLjCCASIdQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMQO/17hUuSP/7m7qG1isjWGfRQuSzwW5AorTVVmfylYahHoFPMiN
9FWMkZHLVadW0FJrAooF3I6dQmc3YkuLWoI/DMaGcbNdaZ6+1YdB+pDB16dXplnHAsFiyhn89=</ds:X509Certificate>

```



```

        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmlsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDYTCCAkmGAWIBAgIBADANBgkqhkiG9w0BAQsFADBLMQswCQYDVQ
          QGEwJVUzELMAkGA1UECAwCTUkxEjAQBGNVBAcMUFubiBBcmJvcjEbmBkGALUECgwSRHVvIFNlY
          3VyaXR5LDBJbMUMB4XDTE5MDQyOTEwMTQxMFOxDTI5MDQyNjEwMTQxMFOwSzELMAkGA1UEBhMVCV
          VMxCzAJBgNVBAGMAk1JMRlWEAYDVQQHDA1Bbm4gQXJib3IxEzEwLW509Certificate/17hUuSP/7m7qGlisjWGfR
          QuSzWw5AorTVVmfy1yaHHoFPMiN9FWMkZHLVAdW0FJrAooF3I6dQmc3YkuLWoI/DMaGcbNDaZ6+1Yd
          B+pDBl6dXpliNHAsFiyhn89+ee06Thys9yxrND8hYwZfQE3aIB/leEymualh08YDd81iD+XtMijSyhO=</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://WIN-BL0P4116VDB/dag/saml2/idp/SingleLogoutService.php"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://WIN-BL0P4116VDB/dag/saml2/idp/SingleLogoutService.php"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>

    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>

    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>

    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>

    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>

    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://WIN-BL0P4116VDB/dag/saml2/idp/SSOService.php"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://WIN-BL0P4116VDB/dag/saml2/idp/SSOService.php"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://WIN-BL0P4116VDB/dag/saml2/idp/SSOService.php"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

Example – Modifying SAML Profile

In the following example, you can use the `samlconfig` command to modify the service provider or identity provider settings of an existing SAML profile.

```
mail.example.com > samlconfig
```

Choose the operation you want to perform:

- UILOGIN - Create a new SAML Profile for UI Login.

```
[ ]> uilogin
```

Currently configured SAML User profiles:

```

-----
-----
-----
Type           Name           Entity ID           URL
-----
SP Settings    SP1             ENTSP               http://mail.example.com
IDP Settings   IDP1            https://WIN-BL0P4116
BL0P4116VDB/dag/saml2/idp/Si
-----
-----

```

```

Choose the operation you want to perform:
- EDIT - Modify a SAML profile.
- DELETE - Delete a SAML profile.
[ ]> edit
Choose the operation you want to perform:
- SP - Edit Service Provider Settings.
- IDP - Edit Identity Provider Settings.
[ ]>

```

settime

Description

The **settime** command allows you to manually set the time if you are not using an NTP server. The command asks you if you want to stop NTP and manually set the system clock. Enter the time is using this format: **MM/DD/YYYY HH:MM:SS**.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```

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

Description

Set the local time zone.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
mail3.example.com> setz
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

Description

Shut down the system to power off

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

- [Description, on page 126](#)
- [Usage, on page 126](#)
- [Example, on page 126](#)

Description

The `smaconfig` command is used to add, delete, or view the Cisco Secure Email and Web Manager connection parameters and keys.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Example

In the following example, you can use the `smaconfig` command to add email gateways to the Cisco Secure Email and Web Manager using pre-shared keys, and view the Cisco Secure Email and Web Manager connection details (host name and user keys).

```
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
-----
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
-----
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

Description

Configure SSH server and user key settings.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to cluster mode.

Batch Command: This command does not support a batch format.

Examples

Example: Editing SSH Server Configuration

The following example shows how to edit the SSH server configuration:

```
mail1.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 allowed list/blocked list
[]> sshd

ssh server config settings:
Public Key Authentication Algorithms:
    rsal
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-cbc
    aes192-cbc
    aes256-cbc
    rijndael-cbc@lysator.liu.se
MAC Methods:
    hmac-shal
Minimum Server Key Size:
    2048
KEX Algorithms:
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-shal
    diffie-hellman-group14-shal
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521

Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup

Available Public Key Authentication Algorithms options :
    rsal
    ssh-dss
    ssh-rsa
```

Example: Editing SSH Server Configuration

```

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>
Available Cipher Algorithms options :
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-cbc
    3des-cbc
    aes192-cbc
    aes256-cbc
    rijndael-cbc@lysator.liu.se

Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,
aes256-cbc,rijndael-cbc@lysator.liu.se]>

Available MAC Methods options :
    hmac-md5
    hmac-shal
    umac-64@openssh.com
    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-shal-96
    hmac-md5-96

Enter the MAC Methods do you want to use
[hmac-shal]>

Available Key Sizes : [768, 1024, 1536, 2048]
Enter the Minimum Server Key Size do you want to use
[2048]>

Available KEX Algorithms options :
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-shal
    diffie-hellman-group14-shal
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-shal,
diffie-hellman-group14-shal,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521]>

ssh server config settings:
Public Key Authentication Algorithms:
    rsa1
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-cbc
    aes192-cbc
    aes256-cbc
    rijndael-cbc@lysator.liu.se
MAC Methods:
    hmac-shal
Minimum Server Key Size:
    2048
KEX Algorithms:
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-shal

```

```
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

```
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

Example: Installing a New Public Key for the Administrator Account

In the following example, a new public key is installed for the administrator account:

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

Example: Categorizing an IP Address as Persistent Blocked List or Allowed List

If the email gateway or the `ipblockd` service is restarted, the IP address that you categorize as a persistent blocked list or allowed list is retained.



Note You can categorize IP addresses as persistent blocked lists\or allowed lists only on AsyncOS 11.0.2 and above.

The following example shows how to categorize IP addresses as persistent allowed list:

```
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 allowed list/blocked list
[]> access control

Choose the operation you want to perform:
- ALLOWED_LIST - Manage the persistent allowed list
- BLOCKED_LIST - Manage the persistent blocked list
[]> allowed_list

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 Allowed list will be ignored.
[]> 10.8.85.77
```

The addresses were successfully added to the Allowed list

The following example shows how to categorize IP addresses as persistent blocked list:

```
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 allowed list/blocked list
[]> access control
```

```
Choose the operation you want to perform:
- ALLOWED_LIST - Manage the persistent allowed list
- BLOCKED_LIST - Manage the persistent blocked list
[]> blocked_list
```

```
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 Allowed list will be ignored.
[]> 10.8.85.77
```

The addresses were successfully added to the blocked list

status

Description

Show system status.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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:                    Reset          Uptime          Lifetime
  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:	Current		
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

Description

Send a message to Cisco customer support. This command requires that the email gateway is able to send mail to the Internet. A trouble ticket is automatically created, or you can associate the support request with an existing trouble ticket.

To access Cisco technical support directly from the email gateway, your Cisco.com user ID must be associated with your service agreement contract for this email gateway. To view a list of service contracts that are currently associated with your Cisco.com profile, visit the Cisco.com Profile Manager at <https://sso.cisco.com/auth/forms/CDClogin.html> . If you do not have a Cisco.com user ID, register to get one. See information about registering for an account in the online help or user guide for your release.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

The following example shows a support request that is not related to an existing support ticket.

```
mail.example.com> supportrequest
Please Note:
If you have an urgent issue, please call one of our worldwide Support Centers
```

Example

```

(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.qa?
[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

Description

Display Support Request Keywords version information for requesting support from Cisco TAC.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

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

supportrequestupdate

Description

Request manual update of Support Request Keywords for requesting support from Cisco TAC.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

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

suspend

Description

Suspend receiving and deliveries

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Suspend deliveries

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Suspend receiving.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Display information about files opened by processes.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Allow Cisco TAC to access your system.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```

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

Description

Establish an outbound TLS connection on demand and debug any TLS connection issues concerning a destination domain. To create the connection, specify the domain to verify against and the destination host. AsyncOS checks the TLS connection based on the Required (Verify) TLS setting

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

The batch format of the `tlsverify` command can be used to perform all the functions of the traditional CLI command to check the TLS connection to the given hostname.

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

Example

```

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 mx.example.com.
TLS verification completed.
```

trace

Description

Trace the flow of a message through the system

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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]>

```



Note When using trace , you must include both the header and the body of the message pasted into the CLI.

trackingconfig

Description

Configure the tracking system.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Example

Batch Command: This command does not support a batch format.

Example

```
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

Description

Update timezone rules

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command supports a batch format.

Batch Format

The batch format of the tzupdate command forces an update off all time zone rules even if no changes are detected.

```
tzupdate [force]
```

Example

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

updateconfig

Description

Configure system update parameters.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Examples

Configure the Email Gateway to Download Updates from Updater Servers

In the following example, the updateconfig command is used to configure the email gateway to download update images from Cisco servers and download the list of available AsyncOS upgrades from a local server.

```
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
[ ]> setup
For the following services, please select where the system will download updates from:
Service (images):                               Update URL:
-----
Feature Key updates                             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                                 Cisco IronPort Servers
Enrollment Client Updates                     Cisco IronPort Servers
Support Request updates                       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
```

Configure the Email Gateway to Download Updates from Updater 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

[N]>
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
[]>

```

Configure the Email Gateway to Verify the Validity of Updater Server Certificate

If you configure this option, every time the email gateway communicates the Cisco updater server, the validity of the updater server certificate is verified. If the verification fails, updates are not downloaded and the details are logged in Updater Logs. The following example shows how to configure this option:

```

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

```

Configure the Email Gateway to Trust Proxy Server Communication

```

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>

```

Configure the Email Gateway to Trust Proxy Server Communication

If you are using a non-transparent proxy server, you can add the CA certificate used to sign the proxy certificate to the email gateway. By doing so, the email gateway trusts the proxy server communication. The following example shows how to configure this option:

```

...
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-----
MMIICiDCCAFgGwAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMakGA1UEBhMCSU4x
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.
[]>

```

Uploading Cisco Talos Certificate in Email Gateway

In the following example, you can use the `updateconfig > clientcertificate` sub command to upload the Cisco Talos certificate in the email gateway

```

maill.example.com> updateconfig

Service (images): Update URL:
-----
Feature Key updates http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions Cisco IronPort Servers
DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Enrollment Client Updates (used to fetch certificates for URL Filtering) Cisco IronPort
Servers
Support Request updates Cisco IronPort Servers
Content Scanner Updates Cisco IronPort Servers
Geo Countries Updates Cisco IronPort Servers
SDR Client Updates Cisco IronPort Servers
External Threat Feeds updates Cisco IronPort Servers
How-Tos Updates Cisco IronPort Servers
Notifications component Updates Cisco IronPort Servers
Smart License Agent Updates Cisco IronPort Servers
Mailbox Remediation Updates Cisco IronPort Servers

```

```
Talos Updates Cisco IronPort Servers
Easy Demo service Updates Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
```

```
Service (list): Update URL:
```

```
-----
McAfee Anti-Virus definitions Cisco IronPort Servers
DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Enrollment Client Updates (used to fetch certificates for URL Filtering) Cisco IronPort
Servers
Support Request updates Cisco IronPort Servers
Content Scanner Updates Cisco IronPort Servers
Geo Countries Updates Cisco IronPort Servers
SDR Client Updates Cisco IronPort Servers
External Threat Feeds updates Cisco IronPort Servers
How-Tos Updates Cisco IronPort Servers
Notifications component Updates Cisco IronPort Servers
Smart License Agent Updates Cisco IronPort Servers
Mailbox Remediation Updates Cisco IronPort Servers
Talos Updates Cisco IronPort Servers
Easy Demo service 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
- CLIENTCERTIFICATE - Upload the client certificate and key.

```
[ ]>clientcertificate
```

```
Do you like to overwrite the existing certificate and key [Y|N] ? [ ]> y
```

```
Paste the certificate.
```

```
Press CTRL-D on a blank line when done.
```

```
-----BEGIN CERTIFICATE-----
```

```
f14wXRnvDRjPWUX8XRHyF8RdLlfz8rh/1xJN6R4V0L1HPAJ5fEyJTmNiT1FcgjrN
Sm57NsyVCoNJ00iCuwi6Hiw/CY1fms99ObtByIrwT5G1+6E6J6qq9ovT6R+qiS2A
KGNIRJAvZNhiDdezX5O21/xbJ5C39BPqgY0CAwEAAaMaMBgwCQYDVR0TBAlwADAL
BgNVHQ8EBID07O4MAOGCSqGSib3DQEBCwUAMHwxCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ueG90Ym90aWwvY291bnQ5LmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAAODerFpMLiDrHCpbqqlZT+3XgIXFaDNAIILMNVnxCv+Cg/8FolhT
mNnefWoKq/CxK9jNfUHaly3BzozOUzFH87gXdNrhFrRnMRqRwBQH1ImKjmf1sogY4
EUC/7+pQ52K8/fulXXMT463BwkXD5R0tr6bTdoUSDfRL3aWhTjdWrX0WolkTp0sR
```

```
f14wXRnvDRjPWUX8XRHyF8RdLlfz8rh/1xJN6R4V0L1HPAJ5fEyJTmNiT1FcggjrN
Sm57NsyVCoNJ0OiCuwi6Hiw/CYlfms99ObtByIrwT5G1+6E6J6qq9ovT6R+qiS2A
KGNIRJAvZnhiDdeZx5021/xBJ5C39BPqgY0CAwEAAaMaMBgwCQYDVROTBAlWADAL
BgNVHQ8EBAMCB4AwDQYJKoNmX8IWBh7WWxaJKGe9d5P62zBCgZcep4PsH
dt396r7VqCRREgZAMV45X1xrK7VMds9+jCa1EW6VOr5PrTPK4uBqqqQCku3RmgWm
7H/W+oYBkj29ny8ULvTPRT/w6KYsgZiTASogHK69IY12We7AiBP+DmNCK9pRBpuk
oWbMf00voF8k2QZf1S3ms17dn7LmOYB+/6e8RR1T+9Y1AkftIm0dLEMxjb32bCh2
4zQQWIXyTxiG5CDuRC+a/P7dZZQnLQfzoscc9w1YSX1T6ns5v4RrL8phX4b0bTA=
-----END CERTIFICATE-----
^D
```

```
Paste Private Key.
Press CTRL-D on a blank line when done.
-----BEGIN RSA PRIVATE KEY-----
```

```
Z1DbPzJm57AODTwUJEFgJ/u/x7bRzw/BFH6QUu8WddbqIgtFhwaqAP2uzB18a38
VvfZxsZff+OvU2hUrznWK5RgsCYILAYpn7shh7Rxp4QJc6hCcEf0731BVgguKfPC
egyztK0stKvXPcbT0T1BwWu8n1vm5UD0I+UjKqiqIniL3MGY0VMVzo2oZ1PFHiVO
JLuMHpI4dvhQoq7UaLoT4NOYeIcC3iykZ0n8BlBzVAY3KVvfazkR7QJwXYSjRqL9
708vImECgYEA/CewuUKZbBrGVGLr+eL34h0uOMgx8+tMFeRnBwMTIHWxcGxJ/bj8
6+LCS9aXfuD0BHDJ+Xy4mfsK0vz5dtpFL5qI71NvN6VUrPI3tIXdUTxZ9HeJKHjN
MIIEpQIBAAKCAQEAA4N6sWjM5TMufzuBd02uF9GcxGpHAFaeUiYqOZ+Wyi
BjgrQL/v61DnYrz9+6VdcxPjrcHCRCpLHS2vptN2hRIN9EvdpaFON1atfRaiWRon
SxF+XjBdGe8NGM9ZRfxdEfiXxF0uV/PyuH/XEk3pHhXQuUc8An18T11OY2JPUVyC
Os1Kbns2zJUKg0nQ6IK7CLOeLD8JiV+az305u0HIivC3kbX7oTonqqr2i9PpH6qJ
LYAoY0hEkC9k2GIN1Bae160AtKWWdKRS13nunfaiFun/XAeF9YPUa24+dc
Z1DbPzJm57AODTwUJEFgJ/u/x7bRzw/BFH6QUu8WddbqIgtFhwaqAP2uzB18a38
VvfZxsZff+OvU2hUrznWK5RgsCYILAYpn7shh7Rxp4QJc6hCcEf0731BVgguKfPC
egyztK0stKvXPcbT0T1BwWu8n1vm5UD0I+UjKqiqIniL3MGY0VMVzo2oZ1PFHiVO
JLuMHpI4dvhQoq7UaLoT4NOYeIcC3iykZ0n8BlBzVAY3KVvfazkR7QJwXYSjRqL9
708vImECgYEA/CewuUKZbBrGVGLr+eL34h0uOMgx8+tMFeRnBwMTIHWxcGxJ/bj8
6+LCS9aXfuD0BHDJ+Xy4mfsK0vz5dtpFL5qI71NvN6VUrPI3tIXdUTxZ9HeJKHjN
r5082sZd0w6W00qjfk1XZowut9isGWJwPMPoY0hWfyxbv7bmFC50AkCgYEA5Ex4
/gvS/ruvJNVaial8uJD6KEeRkYBaBMdoleLLSqyoFj1x/qBBeSm6pvbxSoyaUJ28
kNht392kc6NEq1fW79zdD4wcnkREOcrKfLsjCxyOnrkg7K+TkcrbRDUD0ErAPv3w
sLbnSXTm0DZYUB0xC2utEnkSOHLRrJNaCTs5tmUCgYEA8oZSSb2uxvVxsJR81xog
hVC/tkmHEi5MPfoyxehFMcFBavocqHaWfWLasgqyJ4zB5st82AOHokJ9BLXgUtpZ
FRIZhdal8AWKzdUikvT2Cz5a3vFh8JVQcApyD5Ifh/JNtmyn170+3RkTjixOSxQN
Taeqbx3I5q4w0qs6FuP9YdECgYEAAGCpOYpDQyyEimlakKKR12EfLqIFFP6IG51fr
ZvoDltCHLLUiIghluVer6cAIhgmZOFjVW5u1U2BiymiGTIrrp40erXPDPtAl9qva
MvV9uGc3yf00GcuxdM+leQ0p2ZhdhP+a+Bo2jg6K5akcux0oQ3kXmJ9Pk1EiVPgE
O9p78+ECgYEAarT10KuEKhy4tYNBOQIEc9X5hCod8nfaoRzfzCC9j2C2pKY8bd6Kz
AOQUeQTEXGgVZQq/5CWQOEUYtE6xtkerH80yN0jvcAmm5d2RpJzQu8W6WfyckFEQ
I85GwuImHH5/duK8kJgzXRiTJVEbDYe7WneMHbmgSQbIvfXb02tSG1c=
-----END RSA PRIVATE KEY-----
^D
```

```
Certificate and key are stored successfully
```

updatenow

Description

Requests an update to all system service components.

Usage

Commit: This command does not require a ‘commit’.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command does support a batch format.

Batch Format

The batch format of the `updatenow` command can be used to update all components on the email gateway even if no changes are detected.

```
updatenow [force]
```

Example

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

version

Description

View system version information

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Use the **wipedata** command to wipe the core files on the disk and check the status of the last coredump operation.



Note Depending on the size of the data, wipe action may take a while and can affect the system performance until the action is complete.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

The **upgrade** CLI command displays a list of available upgrades and upgrades the AsyncOS system to the version specified by the user.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
mail3.example.com> upgrade
Are you sure you want to proceed with upgrade? [N]> y

Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[]> downloadinstall

Upgrades available.
1. AsyncOS 10.0.2 build 020 upgrade For Email, 2017-05-09. This is release for Maintenance
   Deployment.
2. AsyncOS 11.0.0 build 132 upgrade For Management, 2017-12-08.This release is for Maintenance
   Deployment.
.....
Performing an upgrade may require a reboot of the system after the upgrade is applied. You
can log in to your appliance after the upgrade is done.
Do you want to proceed with the upgrade? [Y]>Y
```

Content Scanning

contentscannerstatus

Display the content scanning engine version information.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

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

contentscannerupdate

Request manual update of the content scanning engine. If 'force' parameter is used, update is performed even if no changes are detected.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command does not support a batch format.

Example

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

LDAP

This section contains the following CLI commands:

Idapconfig

Description

Configure LDAP servers

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example - Creating a New LDAP Server Profile

In the following example, the `Idapconfig` command is used to define an LDAP server for the email gateway to bind to, and queries for recipient acceptance (`ldapaccept` subcommand), routing (`ldaprouting` subcommand), masquerading (`masquerade` subcommand), end-user authentication for the Spam Quarantine (`isqauth` subcommand), and alias consolidation for spam notifications (`isqalias` subcommand) are configured.

First, the nickname of "PublicLDAP" is given for the `mldapserver.example.com` LDAP server. Queries are directed to port 3268 (the default). The search base of `example.com` is defined (`dc=example,dc=com`), and queries for recipient acceptance, mail re-routing, and masquerading are defined. The queries in this example are similar to an OpenLDAP directory configuration which uses the `inetLocalMailRecipient` auxiliary object class defined in the expired Internet Draft *draft-lachman-laser-ldap-mail-routing-xx.txt* , also sometimes known as "the Laser spec." (A version of this draft is included with the OpenLDAP source distribution.) Note that in this example, the alternate mailhost to use for queried recipients in the mail re-routing query is `mailForwardingAddress` . Remember that query names are case-sensitive and must match exactly in order to return the proper results.

```
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:
[]> mldapserver.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.

```

Example - Creating a New LDAP Server Profile

```

    [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: myldapservers.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: myldapservers.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.
[]>

```

Example - Configuring Global Settings

In the following example, the LDAP global settings are configured, including the certificate for TLS connections.

```

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.
[1]>

```

Idapflush

Description

Flush any cached LDAP results.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```

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

```

Idaptest

Description

Perform a single LDAP query test

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

In this example, the `ldaptest` command is used to test the only recipient acceptance query for the configured LDAP server configuration. The recipient address "admin@example.com" passes the test, while the recipient address "bogus@example.com" fails.

```

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
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

Description

Sets or disables the character used for Sieve Email Filtering, as described in RFC 3598. Note that the Sieve Character is ONLY recognized in LDAP Accept and LDAP Reroute queries. Other parts of the system will operate on the complete email address.

Allowable characters are: `-_=#/+^#`

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

In this example, the sievechar command is used to define + as the sieve character recognized in Accept and LDAP Reroute queries.

```

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.
[]>

```

Mail Delivery Configuration/Monitoring

This section contains the following CLI commands:

addresslistconfig

Description

Configure address lists.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

The batch format for the `addresslistconfig` command can be used to create a new address list, edit an existing address list, print a list of address lists, delete an address list, or find conflicting addresses within an address list.

- Adding a new address list:

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

- Editing an existing address list:

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

- Deleting an address list:

```
addresslistconfig delete <name>
```

- Printing a list of address lists:

```
addresslistconfig print <name>
```

- Finding conflicting addresses within an address list:

```
addresslistconfig conflicts <name>
```

Example

```
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

Description

Configure email aliases.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

The batch format of the aliasconfig command can be used to add a new alias table, edit an existing table, print a list of email aliases, and import/export alias table. To invoke as a batch command, use the following format of the aliasconfig command with the variables listed below:

- Adding a new email alias:

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



Note Using the 'aliasconfig new' command with a non-existent domain causes the domain to be created.

- Editing an existing email alias

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

- Displaying an email alias:

```
aliasconfig print
```

- Importing a local alias listing:

```
aliasconfig import <filename>
```

- Exporting an alias listing on the email gateway:

```
aliasconfig export <filename>
```

Example

```
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.
[ ]>

```

Table 6: Arguments for Configuring Aliases

Argument	Description
<domain>	The domain context in which an alias is applied. 'Global' specifies the Global Domain Context.
<alias>	The name of the alias to configure Aliases permitted at the Global Comain Context: '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. Aliases permitted for specific domain contexts: 'user'— This user in this domain context 'user@domain'— This email address
<email_address>	The email address that an alias mapps to. A single alias can map to multiple email addresses.
<filename>	The filename to use with importing/exporting the alias table.

archivemessage

Description

Archive older messages in your queue.

Usage

Commit: This command does not require a commit.

Cluster Management: This command is restricted to machine mode..

Batch Command: This command does not support a batch format.

Example

In the following example, an older message is archived:

```
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

Description

Configure Virtual Gateway(tm) mappings.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In the following example, the altsrchoost table is printed to show that there are no existing mappings. Two entries are then created:

- Mail from the groupware server host named @exchange.example.com is mapped to the PublicNet interface.
- Mail from the sender IP address of 192.168.35.35 is mapped to the AnotherPublicNet interface.

Finally, the altsrchoost mappings are printed to confirm and the changes are committed.

```
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

Description

Configure the behavior of bounces.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. See the inline CLI help for more details. Use the help command to access the inline help for this command.

Example

In the following example, a bounce profile named bounceprofile is created using the **bounceconfig** command. In this profile, all hard bounced messages are sent to the alternate address **bounce-mailbox@example.com**. Delay warnings messages are enabled. One warning message will be sent per recipient, and the default value of 4 hours (14400 seconds) between warning messages is accepted

```
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>

```

Applying a Bounce Profile to a Listener

After a bounce profile has been configured, you can apply the profile for each listener using the `listenerconfig` -> `bounceconfig` command and then committing the changes.



Note Bounce profiles can be applied based upon the listener that a message was received on. However, this listener has nothing to do with how the message is ultimately delivered.

In this example, the `OutboundMail` private listener is edited and the bounce profile named `bouncepr1` is applied to it.

```

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

Description

Bounce messages from the queue.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

Recipients to be bounced are identified by either the destination recipient host or the message sender identified by the specific address given in the Envelope From line of the message envelope. Alternately, all messages in the delivery queue can be bounced at once.

Bounce by Recipient Host

```
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.
```

Bounce by Envelope From Address

```
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.
```

Bounce All

```
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

Description

Configure settings for Bounce Verification. Use this command to configure keys and invalid bounced emails.

Usage

Commit: This command requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

The following example shows key configuration and settings configured for invalid bounced emails.

```
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

Description

Delete messages from the queue

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

The email gateway gives you various options to delete recipients depending upon the need. The following example show deleting recipients by recipient host, deleting by Envelope From Address, and deleting all recipients in the queue.

Delete by Recipient Domain

```
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.
```

Delete by Envelope From Address

```
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.
```

Delete All

```
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

Description

Configure mail delivery

Usage

Commit: This command requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In the following example, the `deliveryconfig` command is used to set the default interface to “Auto” with “Possible Delivery” enabled. The system-wide maximum outbound message delivery is set to 9000 connections.

```
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

Description

Reschedule messages for immediate delivery. Users have the option of selecting a single recipient host, or all messages currently scheduled for delivery.

Usage

Commit: This command does not require a ‘commit’.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```
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

Formerly the **setgoodtable** command. The table is now called the Destination Control Table. Use this table to configure delivery limits for a specified domain.

Using the destconfig Command

The following commands are available within the destconfig submenu:

Table 7: destconfig Subcommands

Syntax	Description
SETUP	Change global settings.
NEW	Add new limits for a domain.
EDIT	Modify the limits for a domain.
DELETE	Remove the limits for a domain.
DEFAULT	Change the default limits for non-specified domains.
LIST	Display the list of domains and their limits.
DETAIL	Display the details for one destination or all entries.
CLEAR	Remove all entries from the table.
IMPORT	Imports a table of destination control entries from a .INI configuration file.
EXPORT	Exports a table of destination control entries to a .INI configuration file.

The **destconfig** command requires the following information for each row in the Destination Controls table.

- Domain (recipient host)
- Maximum simultaneous connections to the domain
- Messages-per-connection limit
- Recipient limit
- System-wide or Virtual Gateway switch
- Enforce limits per domain

- Time period for recipient limit (in minutes)
- Bounce Verification
- Bounce profile to use for the domain

Sample Destination Control Table

The following table shows entries in a destination control table.

Table 8: Example Destination Control Table Entries

Domain	Conn. Limit	Rcpt. Limit	Min. Prd.	Enforce MX/DOM
(default)	500	None	1	Domain
Unlisted domains get their own set of 500 connections with unlimited repts/hr				
(default)	500	None	1	MXIP
Mail gateways at unlisted domains get up to 500 connections, with unlimited repts/hr				
partner.com	10	500	60	Domain
All gateways at partner.com will share 10 connections, with 500 repts/minute maximum				
101.202.101.2	500	None	0	MXIP
Specifying an IP address				

Batch Format

The batch format of the `destconfig` command can be used to perform all the functions of the traditional CLI command.

- Creating a new destination control table

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

- Editing an existing destination control table

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

- Deleting an existing destination control table

```
destconfig delete <profile>
```

- Displaying a summary of all destination control entries


```
destconfig list
```

- Displaying details for one destination or all entries

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

- Deleting all existing destination control table entries

```
destconfig clear
```

- Import table from a file

```
destconfig import <filename>
```

- Export table to a file

```
destconfig export <filename>
```

For the edit and new batch commands, any or all of the following options may be provided by identifying the value with the variable name and an equals sign. Options not specified will not be modified (if using edit) or will be set to default values (if using new).

`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.

`tls_certid="<certificate>"` - Certificate used for this destination control.

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

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

Example: Creating a new destconfig Entry

In the following example, the current destconfig entries are printed to the screen. Then, a new entry for the domain partner.com is created. The concurrency limit of 100 simultaneous connections and recipient limit of 50 recipients for a 60-minute time period is set for that domain. So, the system will never open more than 100 connections or deliver to more than more than 50 recipients in a given hour to the domain partner.com . No bounce profile is assigned for this specific domain, and no specific TLS setting is configured. Finally, the changes are printed to confirm and then committed

```
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
      Rate          Bounce          Bounce
Domain  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

```

Example: Bounce Profile and TLS Settings

In this example, a new destconfig entry is configured for the domain newpartner.com. TLS connections are required. The example also shows the bounce profile named bouncepr1 (see [Applying a Bounce Profile to a Listener, on page 163](#)) configured to be used for all email delivery to the domain newpartner.com .

```

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 configure a specific certificate for connections to this domain? [Y]>
1. example1.com
2. example.com
Please choose the certificate to apply:
[1]>

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.

```

Example: Inbound “Shock Absorber”

```

- 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.
[> 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

```

Example: Inbound “Shock Absorber”

In this example, another **destconfig** entry is created to throttle mail to the internal groupware server exchange.example.com . This “shock absorber” entry for your internal server throttles inbound delivery to your internal groupware servers during periods of especially high volume traffic. In this example, the email gateway will never open more than ten simultaneous connections or deliver to more than 1000 recipients to the internal groupware server exchange.example.com in any given *minute* . No bounce profile or TLS setting is configured:

```

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

```

Example: Global Settings

In this example, the TLS alert and certificate for TLS connections are configured.

```

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

```

Example: Enabling TLS Connection with DANE Support

```

2. Demo
Please choose the certificate to apply:
[1]> 1
Do you want to send an alert when a required TLS connection fails? [N]> n

```

Example: Enabling TLS Connection with DANE Support

In this example, a new `destconfig` entry is configured for the domain `newpartner.com`, where TLS connections are enabled with "Opportunistic" DANE support.



Note You must select a TLS support option to enable the DANE prompt.

```

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.

[1]> new

Enter the domain you wish to configure.[1]> 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 wish to configure a specific certificate for connections to this domain? [Y]> N

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

Description

Monitor activity for a particular host

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```
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
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
```

Use Control-C to stop the hostrate command.

hoststatus

Description

Get the status of the given hostname.

Usage

Commit: This command does not require a 'commit'.

Example

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```
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

Description

Configure the IronPort Image Analysis settings

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```

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

Description

Displays the mid and headers of the oldest non-quarantine message on the system.

Usage

Commit: This command does not require a commit.

Cluster Management: This command is restricted to machine mode..

Batch Command: This command does not support a batch format.

Example

In the following example, an older messages are displayed:

```
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

Description

Monitor message throughput

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Redirect all messages to another relay host.



Danger Redirecting messages to a receiving domain that has /dev/null as its destination results in the loss of messages. The CLI does not display a warning if you redirect mail to such a domain. Check the SMTP route for the receiving domain before redirecting messages.



Danger 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.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

The batch format of the redirectrecipients command can be used to perform all the functions of the traditional CLI command.

- Redirects all mail to another host name or IP address

```
redirectrecipients host <hostname>
```

Example

The following example redirects all mail to the example2.com host.

```

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

Description

Reset all of the counters in the system

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
mail13.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

removemessage

Description

Attempts to safely remove a message for a given message ID.

The **removemessage** command can only remove messages that are in the work queue, retry queue, or a destination queue. Note that depending on the state of the system, valid and active messages may not be in any of those queues.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Shows the message and message body for a specified message ID.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Show messages from the queue by recipient host, Envelope From address, or all messages.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does support a batch format.

Batch Format

The batch format of the showrecipients command can be used to perform all the functions of the traditional CLI command.

- Find messages by a recipient host name

```
showrecipients host <hostname>
```

- Find messages by an envelope from address

```
showrecipients [sender_options] <sender_email>
```

Example

The following sender_option is available:

--match-case Case-sensitive matching for the username portion of an address.

- Find all messages

```
showrecipients all
```

Example

The following example shows messages in the queue for all recipient hosts.

```
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

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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:
  Receiving
    Messages Received                    2
    Recipients Received                  2
  Rejection
    Rejected Recipients                  0
    Dropped Messages                     0
  Queue
    Soft Bounced Events                 0
  Completion
    Completed Recipients                  0
  Current IDs
    Message ID (MID)                     2
    Injection Conn. ID (ICID)            0
    Delivery Conn. ID (DCID)            13
Gauges:
  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

Description

To get immediate information about the email queue and determine if a particular recipient host has delivery problems — such as a queue buildup — use the `tophosts` command. The `tophosts` command returns a list of the top 20 recipient hosts in the queue. The list can be sorted by a number of different statistics, including active recipients, connections out, delivered recipients, soft bounced events, and hard bounced recipients.

When Threat Defense Connector is enabled, you can view the delivery status of emails to the message intake address under the `the.tdc.queue` destination domain.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

Example

```
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
5	the.tdc.queue	0	0	5	0	0

topin

Description

Display the top hosts by number of incoming connections

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
mail3.example.com> topin

Status as of:                               Sat Aug 23 21:50:54 2003
```

#	Remote hostname	Remote IP addr.	listener	Conn. In
1	mail.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

Description

Update the global unsubscribe list

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In this example, the address `user@example.net` is added to the Global Unsubscribe list, and the feature is configured to hard bounce messages. Messages sent to this address will be bounced; the email gateway will bounce the message immediately prior to delivery.

```
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

Description

Display and/or alter work queue pause status

Usage

Commit: This command does not require a ‘commit’.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```

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

```



Note Entering a reason is optional. If you do not enter a reason, the system logs the reason as “operator paused”.

In this example, the work queue is resumed:

```

mail3.example.com> workqueue
Status: Paused by admin: checking LDAP server
Messages: 1243
Resume the work queue? [Y]> y
Status: Operational
Messages: 1243

```

Networking Configuration / Network Tools

This section contains the following CLI commands:

etherconfig

Description

Configure Ethernet settings, including media settings, NIC pairing, VLAN configuration, and DSR configuration.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Configure the interface. You can create, edit, or delete interfaces. You can enable FTP, change an IP address, and configure Ethernet IP addresses.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

The batch format of the interfaceconfig command can be used to perform all the functions of the traditional CLI command.

- Creating a new interface

interfaceconfig new <name>
<ethernet interface>
<hostname>

<code>--ip=IPv4 Address/Netmask</code>
<code>--ip6=IPv6 Address/Prefix Length</code>
<code>[--ftp[=<port>]]</code>
<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.

- Deleting an interface

```
interfaceconfig delete <name>
```

Example: Configuring an Interface

```
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 configure custom SMTP Hello to use in the SMTP conversation? [N]>
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

Description

Use the **nslookup** command to check the DNS functionality.

The **nslookup** command can confirm that the email gateway is able to reach and resolve hostnames and IP addresses from a working DNS (domain name service) server.

Table 9: nslookup Command Query Types

Query Type	Description
	the host's Internet address
CNAME	the canonical name for an alias
MX	the mail exchanger
NS	the name server for the named zone

Query Type	Description
PTR	the hostname if the query is an Internet address, otherwise the pointer to other information
SOA	the domain's "start-of-authority" information
TXT	the text information

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```
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

Description

Use the netstat command to displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. Note that this version will not support all arguments. Specifically, you cannot use -a, -A, -g, -m, -M, -N, -s. The command was designed to be run in interactive mode, so that you may enter netstat, then choose from five options to report on. You can also specify the interface to listen on and the interval for display.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

```
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

Description

Use the **netstat** command to displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. Note that this version will not support all arguments. Specifically, you cannot use -a, -A, -g, -m, -M, -N, -s. The command was designed to be run in interactive mode, so that you may enter netstat, then choose from five options to report on. You can also specify the interface to listen on and the interval for display.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format

Example

```
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

Description

The ping command allows you to test connectivity to a network host from the email gateway.

Usage

Commit: This command does not require a 'commit'.

Example

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
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.
[1]> 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
```



Note You must use Control-C to end the ping command.

ping6

Description

Ping a network host using IPv6

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
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.
```



Note You must use Control-C to end the `ping6` command.

routeconfig

Description

The `routeconfig` command allows you to create, edit, and delete static routes for TCP/IP traffic. By default, traffic is routed through the default gateway set with the `setgateway` command. However, AsyncOS allows specific routing based on destination.

Routes consist of a nickname (for future reference), a destination, and a gateway. A gateway (the next hop) is an IP address such as 10.1.1.2. The destination can be one of two things:

- an IP address, such as 192.168.14.32
- a subnet using CIDR notation. For example, 192.168.5.0/24 means the entire class C network from 192.168.5.0 to 192.168.5.255.

For IPv6 addresses, you can use the following formats:

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

The command presents a list of all currently configured TCP/IP routes for you to select from using the `edit` and `delete` subcommands.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

The batch format of the `smtproutes` command can be used to perform all the functions of the traditional CLI command. You can choose whether to use IPv4 or IPv6 addresses for the route.

- Creating a static route:

```
routeconfig new 4|6 <name> <destination_address> <gateway_ip>
```

Table 10: routeconfig Arguments

Argument	Description
4 6	The IP version (IPv4 or IPv6) to apply this command to. For clear and print this option can be omitted and the command applies to both versions.
name	The name of the route.
destination_address	The IP or CIDR address to match on for outgoing IP traffic.
gateway_ip	The IP address to send this traffic to.

- Editing a static route:

```
routeconfig edit 4|6 <name> <new_name> <destination_address> <gateway_ip>
```

- Deleting a static route:

```
routeconfig delete 4|6 <name>
```

- Deleting all static routes:

```
routeconfig clear [4|6]
```

- Printing a list of static routes:

```
routeconfig print [4|6]
```

Example

```
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

Description

The setgateway command configures the default next-hop intermediary through which packets should be routed. Alternate (non-default) gateways are configured using the routeconfig command.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

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

Description

The hostname is used to identify the system at the CLI prompt. You must enter a fully-qualified hostname. The sethostname command sets the name of the email gateway. The new hostname does not take effect until you issue the commit command.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

For the hostname change to take effect, you must enter the commit command. After you have successfully committed the hostname change, the new name appears in the CLI prompt:

```
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
```

The new hostname appears in the prompt as follows:

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

smtproutes

Description

Set up permanent domain redirections.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

The batch format of the smtproutes command can be used to perform all the functions of the traditional CLI command.

- Creating a new SMTP route

```
smtproutes new <source> <destination> [destination] [destination] [...]
```

- Deleting an existing SMTP route

```
smtproutes delete <source>
```

- Clear a listing of SMTP routes

```
smtproutes clear
```

- Print a listing of SMTP routes

```
smtproutes print
```

- Import a listing of SMTP routes

```
smtproutes import <filenames>
```

- Export a listing of SMTP routes

```
smtproutes export <filenames>
```

Example

In the following example, the `smtproutes` command is used to construct a route (mapping) for the domain `example.com` to `relay1.example.com`, `relay2.example.com`, and `backup-relay.example.com`. Use `/pri=#` to specify a destination priority. THE # should be from 0-65535, with larger numbers indicating decreasing priority. If unspecified, the priority defaults to 0.

(Note that you may have constructed the same mapping during the `systemsetup` command when you configured the InboundMail public listener.)

```
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

Description

Configure SSL settings for the email gateway.



Note You cannot change server and client methods in the FIPS 140-2 compliance mode.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

mail.example.com> sslconfig

sslconfig settings:
  GUI HTTPS method:  tlsv1_1tlsv1_2
  GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
  GUI HTTPS TLS Renegotiation: Enabled

  Inbound SMTP method:  tlsv1_1tlsv1_2
  Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA

```



```

!aNULL
!kRSA
@STRENGTH
-aNULL
-EXPORT
-IDEA
Inbound SMTP TLS Renegotiation: Enabled

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
  !kRSA
  @STRENGTH
  -aNULL
  -EXPORT
  -IDEA
Other TLS Client Services: TLS v1.2, TLS v1.1 are being used as default

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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
[]> gui
Enter the GUI HTTPS ssl method you want to use.
1. TLS v1.1
2. TLS v1.2
3. TLS v1.0

[1, 2]> 1

Enter the GUI HTTPS ssl cipher you want to use.
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:
!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA]>

Would you like to Enable/Disable TLS Renegotiation for GUI HTTPS? [Y]>

sslconfig settings:
GUI HTTPS method: tlsv1_1
GUI HTTPS ciphers:
  AES128
  AES256
  !SRP
  !AESGCM+DH+aRSA
  !AESGCM+RSA
  !aNULL
  !kRSA
  @STRENGTH
  -aNULL
  -EXPORT
  -IDEA
GUI HTTPS TLS Renegotiation: Enabled

```

Example

```

Inbound SMTP method:  tlsv1_1tlsv1_2
Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    Inbound SMTP TLS Renegotiation: Enabled

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
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    Other TLS Client Services: TLS v1.2, TLS v1.1 are being used as default

```

```

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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
[ ]> inbound

```

Enter the inbound SMTP ssl method you want to use.

1. TLS v1.1
2. TLS v1.2
3. TLS v1.0

```
[1, 2]> 2
```

Enter the inbound SMTP ssl cipher you want to use.

```
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:
!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA]>
```

Would you like to Enable/Disable TLS Renegotiation for inbound SMTP? [Y]>

```

sslconfig settings:
GUI HTTPS method:  tlsv1_1
GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL

```

```

!kRSA
@STRENGTH
-aNULL
-EXPORT
-IDEA
GUI HTTPS TLS Renegotiation: Enabled

Inbound SMTP method: tlsv1_2
Inbound SMTP ciphers:
  AES128
  AES256
  !SRP
  !AESGCM+DH+aRSA
  !AESGCM+RSA
  !aNULL
  kRSA
  @STRENGTH
  -aNULL
  -EXPORT
  -IDEA
Inbound SMTP TLS Renegotiation: Enabled

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
  !kRSA
  @STRENGTH
  -aNULL
  -EXPORT
  -IDEA
Other TLS Client Services: TLS v1.2, TLS v1.1 are being used as default

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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
[ ]>

mail1.example.com> sslconfig

sslconfig settings:
GUI HTTPS method:  tlsv1_1tlsv1_2
GUI HTTPS ciphers:
  AES128
  AES256
  !SRP
  !AESGCM+DH+aRSA
  !AESGCM+RSA
  !aNULL
  !kRSA
  @STRENGTH
  -aNULL
  -EXPORT

```

Example

```

        -IDEA
        !DHE-RSA-AES256-SHA
GUI HTTPS TLS Renegotiation: Enabled
Inbound SMTP method:  tlsv1_1tlsv1_2
Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
Inbound SMTP TLS Renegotiation: Enabled
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
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
Other TLS Client Services: TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation: Disabled
Peer Certificate X509 Validation: Disabled

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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, Outbound
SMTP, updater and LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, Outbound
SMTP, updater and LDAP.
[ ]> gui

Enter the GUI HTTPS ssl method you want to use.
1. TLS v1.1
2. TLS v1.2
3. TLS v1.0
[1, 2]> 1

Enter the GUI HTTPS ssl cipher you want to use.
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA]>

Would you like to Enable/Disable TLS Renegotiation for GUI HTTPS? [Y]>

sslconfig settings:

```

```

GUI HTTPS method:  tlsv1_1
GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
GUI HTTPS TLS Renegotiation: Enabled
Inbound SMTP method:  tlsv1_tlsv1_2
Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
Inbound SMTP TLS Renegotiation: Enabled
Outbound SMTP method:  tlsv1_tlsv1_2
Outbound SMTP ciphers:
    ECDH+aRSA
    ECDH+ECDSA
    DHE+DSS+AES
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !eNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
Other TLS Client Services: TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation: Disabled
Peer Certificate X509 Validation: Disabled

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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, Outbound
SMTP, updater and LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, Outbound
SMTP, updater and LDAP.
[ ]> inbound

```

Example

```

Enter the inbound SMTP ssl method you want to use.
1. TLS v1.1
2. TLS v1.2
3. TLS v1.0
[1, 2]> 2

Enter the inbound SMTP ssl cipher you want to use.
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA]>

Would you like to Enable/Disable TLS Renegotiation for inbound SMTP? [Y]>

sslconfig settings:
  GUI HTTPS method:  tlsv1_1
  GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
  GUI HTTPS TLS Renegotiation: Enabled
  Inbound SMTP method:  tlsv1_2
  Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
  Inbound SMTP TLS Renegotiation: Enabled
  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
    !kRSA
    @STRENGTH
    -aNULL
    -EXPORT
    -IDEA
    !DHE-RSA-AES256-SHA
  Other TLS Client Services: TLS v1.2, TLS v1.1 are being used as default
  Peer Certificate FQDN Validation: Disabled
  Peer Certificate X509 Validation: Disabled

```

```
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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, Outbound
SMTP, updater and LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, Outbound
SMTP, updater and LDAP.
[ ]>
```

telnet

Description

Connect to a remote host

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Use the traceroute command to test connectivity to a network host using IPV4 from the email gateway and debug routing issues with network hops.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
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>
```

traceroute6

Description

Use the **traceroute6** command to test connectivity to a network host using IPV6 from the email gateway and debug routing issues with network hops.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
mail.example.com> traceroute6
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
vml0esa0031.qa> traceroute6
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.
traceroute6 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 traceroute6: wrote example.com 12 chars, ret=-1
  *sendto: No route to host
traceroute6: wrote example.com 12 chars, ret=-1
  *sendto: No route to host
traceroute6: wrote example.com 12 chars, ret=-1
```

trailblazerconfig

- [Description, on page 211](#)
- [Usage, on page 211](#)
- [Example, on page 212](#)

Description

The `trailblazerconfig` command is used to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.

You can see the inline help by using the following command on the CLI: `help trailblazerconfig`.



Note By default, `trailblazerconfig` CLI command is enabled on your email gateway. Make sure that the HTTPS ports are opened on the firewall. Also, ensure that your DNS server can resolve the hostname that you specified for accessing the email gateway.

The `trailblazerconfig` command helps you to avoid the following issues:

- Requiring to add multiple certificates for API ports in certain browsers.
- Redirecting to the legacy web interface when you refresh the Spam Quarantine, Safelist or Blocklist page.
- Metrics bar on the Advanced Malware Protection report page does not contain any data.

Important

When you enable `trailblazerconfig` command on the email gateway, the requested URL will contain the `trailblazerconfig` HTTPS port number appended to the hostname.

The syntax is as follows:

```
trailblazerconfig enable <https_port> <http_port>- runs the trailblazer configuration on the default
ports (HTTPS: 4431).
```

```
trailblazerconfig disable- disables the trailblazer configuration
```

```
trailblazerconfig status- checks the status of the trailblazer configuration
```

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

The following example shows how to enable and view status of `trailblazerconfig` command.

```
mail1.example.com> trailblazerconfig enable 4431

trailblazer is enabled.
To access the Next Generation web interface, use the port 4419 for HTTPS.
mail1.example.com> trailblazerconfig status
trailblazer is running with https on 4419 port.
mail1.example.com> trailblazerconfig disable
trailblazer is disabled.
[]>
```

Outbreak Filters

This section contains the following CLI commands:

outbreakconfig

Description

Use the **outbreakconfig** command to configure the Outbreak Filter feature. You perform the following actions using this command:

- Enable Outbreak Filters globally
- Enable Adaptive Rules scanning
- Set a maximum size for files to scan (note that you are entering the size in *bytes*)
- Enable alerts for the Outbreak Filter

Usage

Commit: This command requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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]>

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

Description

Clear the cached Outbreak Rules.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

The **outbreakstatus** command shows the current Outbreak Filters feature settings, including whether the Outbreak Filters feature is enabled, any Outbreak Rules, and the current threshold.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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

Description

Requests an immediate update of CASE rules and engine core.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

Batch Command: This command does not support a batch format.

Example

```
elroy.run> outbreakupdate
Requesting updates for Outbreak Filter Rules.
```

Policy Enforcement

This section contains the following CLI commands:

dictionaryconfig

Description

Configure content dictionaries

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

Use **dictionaryconfig -> new** to create dictionaries, and **dictionaryconfig -> delete** to remove dictionaries.

Creating a Dictionary

```
example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.

[]> 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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- 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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
[]>
```

Creating a Dictionary 2

In this example, a new dictionary named “secret_words” is created to contain the term “codename.” Once the dictionary has been entered, the edit -> settings subcommand is used to define the case-sensitivity and word boundary detection for words in the dictionary.

```
mail3.example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
[> 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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- 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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- 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

```

Importing Dictionaries

In the example below, using the **dictionaryconfig** command, 84 terms in the profanity.txt text file are imported as Unicode (UTF-8) into a dictionary named profanity .

```

mail3.example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
[]> 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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- RENAME - Change the name of a content dictionary.

```

Exporting Dictionaries

In the example below, using the `dictionaryconfig` command, the `secret_words` dictionary is exported to a text file named `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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- 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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- 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
```

Example - Configuring Maximum Number of Content Dictionaries in Email Gateway

In the following example, you can use the `dictionaryconfig>dictionarylimits` sub command to configure a maximum number of 150 content dictionaries in your email gateway.



Note By default, you can configure a maximum of 100 content dictionaries in your email gateway.



Note When you use content dictionaries extensively with 'Message Body or Attachments' content filter condition or 'Body Scanning' or 'Attachment Scanning' message filter rules, it may degrade system performance.

```
mail1.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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- RENAME - Change the name of a content dictionary.
[ ]> dictionarylimits

Enter the maximum number of content dictionaries that you want to create in
your email gateway.
When you use content dictionaries extensively with 'Message Body or
Attachments' content filter condition or 'Body Scanning' or 'Attachment
Scanning' message filter rules, it may degrade system performance.
[100]> 150

The maximum number of content dictionaries that you can configure in your email
gateway is 150.
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.
- DICTIONARYLIMITS - Configure maximum number of content dictionaries that you
can create in your email gateway.
- RENAME - Change the name of a content dictionary.
[ ]>
mail1.example.com> commit

Please enter some comments describing your changes:
[ ]> Committed the new changes

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Aug 05 10:35:10 2021 GMT
mail1.example.com>>
```

exceptionconfig

Description

Use the **exceptionconfig** command in the CLI to create the domain exception table. In this example, the email address “admin@zzzaazzz.com” is added to the domain exception table with a policy of “Allow.”

Usage

Commit: This command requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine)..

Batch Command: This command does not support a batch format.

Example

```
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

Description

Configure message processing options.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

In this example, the filter command is used to create three new filters:

- The first filter is named **big_messages**. It uses the body-size rule to drop messages larger than 10 megabytes.
- The second filter is named **no_mp3s**. It uses the attachment-filename rule to drop messages that contain attachments with the filename extension of .mp3 .
- The third filter is named **mailfrompm**. It uses mail-from rule examines all mail from postmaster@example.com and blind-carbon copies administrator@example.com .

Using the **filter -> list** subcommand, the filters are listed to confirm that they are active and valid, and then the first and last filters are switched in position using the move subcommand. Finally, the changes are committed so that the filters take effect.

```
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

Description

Configure per recipient or sender based policies.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Examples

Creating an Incoming Mail Policy to Drop Spam Messages and Archive Suspected Spam Messages

In this example, the `policyconfig -> edit -> antispm` subcommand is used to edit the Anti-Spam settings for the default incoming mail policy. (Note that this same configuration is available in the GUI from the Email Security Manager feature.)

- First, messages *positively* identified as spam are chosen not to be archived; they will be dropped.
- Messages that are *suspected* to be spam are chosen to be archived. They will also be sent to the Spam Quarantine installed on the server named `quarantine.example.com`. The text `[quarantined: possible spam]` is prepended to the subject line and a special header of `X-quarantined: true` is configured to be added to these suspect messages. In this scenario, Administrators and end-users can check the quarantine for false positives, and an administrator can adjust, if necessary, the suspected spam threshold.

Finally, the changes are committed.

```
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

[]> **antis spam**

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?

Creating a Policy for the Sales Team

```
[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
```

Creating a Policy for the Sales Team

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

[1]> **new**

Enter the name for this policy:

[1]> **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:

[1]> **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**

Creating a Policy for the Engineering Team

```

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

```

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
[]>

```

Then, create the policy for the engineering team (three individual email recipients), specifying that .dwg files are exempt from Outbreak Filter scanning.

Creating a Policy for the Engineering Team

```

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

Creating the scan_for_confidential Content Filter

```

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
[]>

```

Next, create three new content filters to be used in the Incoming Mail Overview policy table.

In the CLI, the filters subcommand of the policyconfig command is the equivalent of the Incoming Content Filters GUI page. When you create content filters in the CLI, you must use the save subcommand to save the filter and return to the policyconfig command.

First, create the scan_for_confidential content filter:

Creating the scan_for_confidential Content 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
[]> 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
[]>

```

Creating the no_mp3s and ex_employee Content Filters

```

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:
[> 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
[> 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
[> new
Enter a name for this filter:
[> ex_employee
Enter a description or comment for this filter (optional):
[> 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
[> 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 File Hash
9. Attachment Name
10. Attachment MIME Type
11. Attachment Protected

```

```

12. Attachment Unprotected
13. Attachment Corrupt
14. Envelope Recipient Address
15. Envelope Recipient in LDAP Group
16. Envelope Sender Address
17. Envelope Sender in LDAP Group
18. Reputation Score
19. Remote IP
20. DKIM authentication result
21 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. Drop Attachments By Hash
15. Send To System Quarantine
16. Duplicate And Send To System Quarantine
17. Add Log Entry
18. Drop (Final Action)
19. Bounce (Final Action)
20. Skip Remaining Content Filters (Final Action)
21. Encrypt (Final Action)
22. Encrypt on Delivery
23. 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. Drop Attachments By Hash
15. Send To System Quarantine
16. Duplicate And Send To System Quarantine
17. Add Log Entry
18. Drop (Final Action)
19. Bounce (Final Action)
20. Skip Remaining Content Filters (Final Action)
21. Encrypt (Final Action)
22. Encrypt on Delivery
23. 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
[ ]>

```

Enabling Content Filters for Specific Policies

The following illustrates how to enable the policies once again to enable the content filters for some policies, but not for others.

```

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
```

Enabling Content Filters for Specific Policies

```

- 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
[]>
```



Note The CLI does not contain the notion of adding a new content filter within an individual policy. Rather, the filters subcommand forces you to manage all content filters from within one subsection of the policyconfig command. For that reason, adding the drop_large_attachments has been omitted from this example.

DLP Policies for Default Outgoing Policy

This illustrates how to enable DLP policies on the default outgoing policy.

```
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
```

Create an Incoming Policy to Drop the Messages Identified as Bulk Email or Social Network Email

```

- OUTBREAK - Modify Outbreak Filters policy
- 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
[ ]>

```

Create an Incoming Policy to Drop the Messages Identified as Bulk Email or Social Network Email

```

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
[ ]>
```

Configure an Incoming Policy to Handle Messages Marked as Unscannable by AMP Engine

```
mail.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
```

Configure an Incoming Policy to Handle Messages Marked as Unscannable by AMP Engine

```

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

```

Example: Setting Priority for "From" Header

In the following example, the `policyconfig > match headers priority` sub command is used to set the priority for the "From" message header, to match the incoming and outgoing messages in your email gateway.

```

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:
-----   -

```

Modify Incoming Policy to Enable Forwarding of Message Metadata to the Cisco Advanced Phishing Protection Cloud Service

```
P1      Envelope Sender
P2      "From" Header
```

Modify Incoming Policy to Enable Forwarding of Message Metadata to the Cisco Advanced Phishing Protection Cloud Service

In the following example, you can create an incoming mail policy to enable forwarding of metadata of messages to the Cisco Advanced Phishing Protection cloud service.

```
mail.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]> 1
```

```
Incoming Mail Policy Configuration
```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----	Advanced Phishing Protection: -----
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled	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: -----	Advanced Phishing Protection: -----
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled	Off

```
Enter the name or number of the entry you wish to edit:[ ]> 1
```

```
Policy Summaries:
```

```
Content Filters: Off (No content filters have been created)
Advanced Phishing Protection: Off
Choose the operation you want to perform:
```

- ADVANCEDPHISHING - Modify Advanced Phishing Protection Policy
- FILTERS - Modify filters

```
[ ]> advancedphishing
```

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

```
- ENABLE - Enable Advanced Phishing Protection Policy

[ ]> enable

Do you want to perform email forwarding [N]> Y

Policy Summaries:
Content Filters: Off (No content filters have been created)
Advanced Phishing Protection: Email Forwarding - enabled

Choose the operation you want to perform:
- ADVANCEDPHISHING - Modify Advanced Phishing Protection Policy
```

Modify Incoming Policy to Drop Message Attachments with File Analysis Verdict Pending

In the following example, you can modify an incoming mail policy to drop message attachments with file analysis verdict still pending.

```
mail1.example.com> policyconfig
Would you like to configure Incoming Mail Policy or Outgoing Mail Policies or Match Headers
Priority?
1. Incoming Mail Polices
2. Outgoing Mail Policies
3. Match Headers Priority
[1]> 1
Incoming Mail Policy Configuration
```

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
-----	-----	-----	-----	-----	-----	-----
DEFAULT	Off	N/A	Enabled	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	Enable	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 (No content filters have been created)
```

Modify Incoming Policy to Drop Message Attachments with File Analysis Verdict Pending

```

Choose the operation you want to perform:
- 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]>

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]>
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]>
Malware Infected Message Handling
Current actions to take if any of the file contains malware and cannot be
repaired:
- Dropping Infected Messages
- Archiving copies of the original message.
Do you want to edit the actions for Malware Infected Message Handling? [N]>

Do you want to edit the actions for Messages with File Analysis Pending? [Y]>

1. Quarantine
2. Deliver As Is
Action applied to the original message:
[2]>

Do you want to deliver mail to an alternate mailhost? [N]>

Do you want to redirect mail to an alternate email address? [N]>

Do you want to add a custom header? [N]>

Do you want to modify the subject? [Y]>

1. Prepend
2. Append

```

```

Select position of text:
[1]>

Enter the text to add:
[[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]]>

Do you want to archive the original message? [Y]>

Do you want to drop attachments with the file analysis verdict still pending? [N]> yes
Messages with File Analysis Pending
Current actions to take if any of the attachments uploaded for file analysis :
- WARNING: Delivering File Analysis Pending messages normally
- Prepending subjects with "[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]"
- Archiving copies of the original message.
- Dropping Attachments with File Analysis Pending.

Mailbox Auto Remediation (MAR) - Disabled
Do you want to disable Mailbox Auto Remediation action? [N]>

Do you want to edit Mailbox Auto Remediation action? [N]>

Advanced-Malware configuration complete

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 (No content filters have been created)

Choose the operation you want to perform:
- ADVANCEDMALWARE - Modify Advanced Malware Protection policy
- FILTERS - Modify filters
[ ]>

```

Creating Content Filter Action to Add Custom Log Entry for Consolidated Event Logs

In the following example, you can use the Add CEF Log Entry content filter action to add a custom log entry for Consolidated Event Logs.

```

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]>

Incoming Mail Policy Configuration
Name: Anti-Spam: Anti-Virus: Advanced Malware Protection: Graymail:
Content Filter: Outbreak Filters:
Advanced Phishing Protection
-----
-----
-----
DEFAULT N/A N/A N/A N/A
Enabled 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

[> **filters**

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:

[> **custom-headers-cel**

Enter a description or comment for this filter (optional):

[> logging custom headers to Consolidated Event Logs

Filter Name: custom-headers-cel

Conditions:

Always Run

Actions:

No actions defined yet.

Description:

logging custom headers to Consolidated Event Logs

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. Edit Header Text

9. FED Action

10. Add CEF Log Entry

11. Send From Specific IP Interface

12. Drop Attachments By Content

13. Drop Attachments By Name

14. Drop Attachments By MIME Type

15. Drop Attachments By File Type

16. Drop Macro-Enabled Attachments

17. Drop Attachments By Size

18. Safe Print Attachments

19. Drop Attachments By Image Analysis Verdict

20. Send To System Quarantine

21. Duplicate And Send To System Quarantine

22. Add Log Entry

```

23. Drop (Final Action)
24. Bounce (Final Action)
25. Skip Remaining Content Filters (Final Action)
26. Encrypt (Final Action)
27. Encrypt on Delivery
28. Skip Outbreak Filters check
29. Replace URLs within message body based on category
30. Defang URLs within message body based on category
31. Redirect URLs within message body to Cisco Security proxy
32. Strip attachments containing URLs based on category
33. Replace URLs within message body and strip attachments (optional) containing URLs based
    on reputation
34. Defang URLs within message body and strip attachments (optional) based on reputation
35. Redirect URLs within message body to Cisco Security Proxy and strip attachments (optional)
    containing URLs based on
reputation
36. Strip attachments containing URLs based on reputation
37. Skip DomainKeys/DKIM Signing
38. S/MIME Gateway sign/encrypt (Final Action)
39. S/MIME Gateway sign/encrypt on Delivery
[1]> 10

Enter a label for the CEF log entry:
[ ]> mylabel

Enter a value for the CEF log entry:
[ ]> myvalue

Filter Name:  custom-headers-cel

Conditions:
Always Run

Actions:
cef-log-entry("mylabel", "myvalue")

Description:
logging custom headers to cef log

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- SAVE - Save filter
[ ]> save

Defined filters:
1. custom-headers-cel: logging custom headers to Consolidated Event Logs

```

quarantineconfig

Description

Configure system quarantines.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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.
```

Users and Quarantines

Once you answer “y” or yes to the question about adding users, you begin user management, where you can manage the user list. This lets you add or remove multiple users to the quarantine without having to go through the other quarantine configuration questions. Press Return (Enter) at an empty prompt ([]>) to exit the user management section and continue with configuring the quarantine.



Note You will only be prompted to give users access to the quarantine if guest or operator users have already been created on the system.

A quarantine's user list only contains users belonging to the Operators or Guests groups. Users in the Administrators group always have full access to the quarantine. When managing the user list, the NEW command is suppressed if all the Operator/Guest users are already on the quarantine's user list. Similarly, DELETE is suppressed if there are no users to delete.

scanconfig

Description

Configure attachment scanning policy

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Example

In this example, the scanconfig command sets these parameters:

- MIME types of video/*, audio/*, image/* are skipped (not scanned for content).
- Nested (recursive) archive attachments up to 10 levels are scanned. (The default is 5 levels.)
- The maximum size for attachments to be scanned is 25 megabytes; anything larger will be skipped. (The default is 5 megabytes.)
- The document metadata is scanned.
- Attachment scanning timeout is set at 180 seconds.
- Attachments that were not scanned are assumed to not match the search pattern. (This is the default behavior.)
- ASCII encoding is configured for use when none is specified for plain body text or anything with MIME type plain/text or plain/html.



Note When setting the assume the attachment matches the search pattern to Y, messages that cannot be scanned will cause the message filter rule to evaluate to true. This could result in unexpected behavior, such as the quarantining of messages that do not match a dictionary, but were quarantined because their content could not be correctly scanned. This setting does not apply to DLP scanning.

```
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.
[ ]> setup
```

Example: Configuring Message Handling Actions for Unscannable Messages

```

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/*

```

Example: Configuring Message Handling Actions for Unscannable Messages

In the following example, the `scanconfig > setup` command is used to enable and configure message handling actions for messages that are not scanned by the Content Scanner because of an attachment extraction failure.

```

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
[ ]> 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

Description

Define a list of message headers to remove.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

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

Description

Configure text resources such as anti-virus alert templates, message disclaimers, and notification templates, including DLP, bounce, and encryption notifications.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

Use **textconfig -> NEW** to create text resources, and **textconfig > delete** to remove them.

```
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.
[ ]>

```

Use **textconfig -> EDIT** to modify an existing text resource. You can change the encoding or replace the text of the selected text resource.

Importing Text Resources

Use **textconfig -> IMPORT** to import a text file as a text resource. The text file must be present in the configuration directory on the email gateway.

```

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.
[]>
```

Exporting Text Resources

Use **textconfig -> EXPORT** to export a text resource as a text file. The text file will be created in the configuration directory on the email gateway.

```
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.
[]>
```

Logging and Alerts

This section contains the following CLI commands:

alertconfig

Description

Configure email alerts.

Usage

Commit: This command requires a 'commit'.

Example: Creating a New Alert

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example: Creating a New Alert

In this example, a new alert recipient (alertadmin@example.com) is created and set to receive critical system, hardware, and directory harvest attack alerts.

```

maill.example.com> 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.
[ ]>

```

Example: Sending Alerts over TLS

In this example, you can use the `alertconfig > setup` sub command to configure your email gateway to send alerts over TLS.


```
mail1.example.com> alertconfig
Sending alerts to:
  admin@company.com
    Class: Outbreak Filters - Severities: All
    Class: Threatfeeds - Severities: All
    Class: SAML - Severities: All
    Class: Message Delivery - Severities: All
    Class: System - Severities: All
    Class: Anti-Virus - Severities: All
    Class: Hardware - Severities: All
    Class: Updater - Severities: All
    Class: AMP - Severities: All
    Class: Anti-Spam - Severities: All
    Class: Release and Support Notifications - Enabled

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: Enabled
You will receive a copy of the weekly AutoSupport reports.

Alert messages are sent using a TLS connection.

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.
[]> setup

Initial number of seconds to wait before sending a duplicate alert.
Enter a value of 0 to disable duplicate alert summaries.
[300]>

Maximum number of seconds to wait before sending a duplicate alert:
[3600]>

Would you like to enable Cisco IronPort AutoSupport, which automatically
emails system alerts and weekly status reports directly to Cisco IronPort
Customer
Support? (Enabling AutoSupport is recommended.) [Y]>

Would you like to receive a copy of the weekly AutoSupport reports? [Y]>

Maximum number of alerts to save:
[50]>

Choose the default interface to be used to deliver alerts
1. Auto
2. Management (10.8.159.11/24: mail1.example.com)
[1]>

Do you want to enable TLS support to send alert messages? [Y]> yes

Sending alerts to:
  admin@company.com
    Class: Outbreak Filters - Severities: All
    Class: Threatfeeds - Severities: All
    Class: SAML - Severities: All
```

```

Class: Message Delivery - Severities: All
Class: System - Severities: All
Class: Anti-Virus - Severities: All
Class: Hardware - Severities: All
Class: Updater - Severities: All
Class: AMP - Severities: All
Class: Anti-Spam - Severities: All
Class: Release and Support Notifications - Enabled

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: Enabled
You will receive a copy of the weekly AutoSupport reports.

Alert messages are sent using a TLS connection.

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

Description

Display the last n alerts sent by the email gateway.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

> 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

Description

Find events in mail log files

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example: Search by envelope FROM

```
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.
[]> "
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
```

Example: Search by Message ID

```
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
-----
```

Example: Search by Subject

```

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

```

Example: Search by Subject

```

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.
[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]> 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

```

Example: Search by envelope TO

```

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.
[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

```

grep

Description

Searches for text in a log file.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

The grep command can be used to search for text strings within logs. Use the following syntax when you run the grep command:

```
grep [-C count] [-e regex] [-i] [-p] [-t] [regex] log_name
```



Note You must enter either `-e regex` or `regex` to return results.

Use the following options when you run the grep command:

Table 11: grep Command Options

Option	Description
-C	Provides lines of context around the grep pattern found. Enter a value to specify the number of lines to include.
-e	Enter a regular expression.
-i	Ignores case sensitivities.
-p	Paginates the output.
-t	Runs the grep command over the tail of the log file.
regex	Enter a regular expression.

Example of grep

The following example shows a search for the text string 'clean' or 'viral' within the antivirus logs. The **grep** command includes a regex expression:

```
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

Description

Configure access to log files.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example of FTP Push Log Subscription

In the following example, the **logconfig** command is used to configure a new delivery log called `myDeliveryLogs`. The log is then configured to be pushed via FTP to a remote host

```

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. "euggui_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]> 8
Please enter the name for the log:
[ ]> 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:
[ ]> 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
```

Example of SCP Push Log Subscription

```

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

```

Example of SCP Push Log Subscription

In the following example, the **logconfig** command is used to configure a new delivery log called LogPush. The log is configured to be pushed via SCP to a remote host with the IP address of 10.1.1.1, as the user logger, and stored in the directory /tmp. Note that the **sshconfig** command is automatically called from within the **logconfig** command when the log retrieval method is SCP push. (See “Configuring Host Keys” for information about Host keys, and “Managing Secure Shell (SSH) Keys” for more information about User keys, in the *User Guide for AsyncOS for Cisco Secure Email Gateway*.) Also note that an IP address can be used at the hostname prompt.

```

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]> 3
Please enter the name for the log:
[1]> LogPush
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 3
Hostname to deliver the logs:
[1]> 10.1.1.1
Port to connect to on the remote host:
[22]>
Username on the remote host:
[1]> logger
Directory on remote host to place logs:
[1]> /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
```

Example of Syslog Push Log Subscription

```

10.1.1.1 ssh-dss
AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwEsArt9LVE2ts5yE9JBTSdUwLvoq0G3FRqiFrce92zgyHtc/
ZWyXavUTIM3XdIbpiEcsMp2XKpSnPPx2ly8bqkpJsSCQcM8zZMDjnOPm8ghiwHXyh7oNEUJCCPnPxAy44r1J5Yz4x9eIoALpOdHUOGR
+j1NAAAFQDQi5GY/X9P1DM3fPMvEx7wc0edlwAAAIb9cgMTEFP1WTAGr1RtbowZP5zWZtVDTxLhdXzjlo4+hb4hBR7DKuc80+naAFnThyH/
J8R3WLJVF79M5gKJbXzuJGDK3Zwl3UyefPqBq201zLQOSJYx1WwWyz/rooqNlBnF4sh12mtq3tde1176QgtwaQA4wK015k3zOWsPwAAAIaIcRYat3y+Blv/
V6wde6BBk+oULv3eK38gafuip4WMBxkG9G06EQi8nss82oznwMBY/pITRQfh4MBmlxTF4VEY00sARrLZtuUUC1QCQvCgh7Nd3YNais2CSbEKBEAIOTF6+
SX2RNpcUF3Wg5ygw92xtqQPKMcZeLtK2ZJRkhC+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 AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwE...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:dss
4. All
[4]> 4
SSH1:rsa
10.1.1.1 1024 35
122606420764474441178474079962066753259278682648965870690129496065430424463013457294798980627829828033793152226
4486945143162182728144539869316125082823280088157400721099756323564785321288161878068307463282343277810013112817667266624451119
1783747965898000855947022484692079466697707373948871554575173520565607

```

Example of Syslog Push Log Subscription

In the following example, the **logconfig** command is used to configure a new delivery log called MailLog SyslogPush . The log is configured to be pushed to a remote syslog server with the IP address of 10.1.1.2, using TCP, with a 'mail' facility and stored in the directory.

```

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

Example: Adding a Custom Log Header to Consolidated Event Logs

```

[1]> 4
Hostname to deliver the logs:
[]> 10.1.1.2

Port to connect to the remote host:
[514]> 514

Which protocol do you want to use to transfer the log data?
1. UDP
2. TCP
[1]> 2

Maximum message size for syslog push:
[1024]> 1024

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
Do you want to transfer the log data from your email gateway
to the syslog server via TLS? [N]> yes
Do you want to enable syslog disk buffer? [N]> yes
Maximum disk buffer size (in bytes) for syslog push:
[100M]>10G
Currently configured logs:
1. "MailLogSyslogPush" Type: "IronPort Text Mail Logs" Retrieval: Syslog Push -
Host 10.1.1.2

```

Example: Adding a Custom Log Header to Consolidated Event Logs

In the following example, you can use the `logconfig > ceflogheaders` sub command to add a custom log header to Consolidated Event Logs.

```
mail11.example.com> logconfig
```

```
Currently configured logs:
```

Log Name	Log Type	Retrieval	Interval
1. amp	AMP Engine Logs	Manual Download	None
2. amparchive	AMP Archive	Manual Download	None
3. antis spam	Anti-Spam Logs	Manual Download	None
4. antivir us	Anti-Virus Logs	Manual Download	None
5. asarchive	Anti-Spam Archive	Manual Download	None
6. authentication	Authentication Logs	Manual Download	None
7. avarchive	Anti-Virus Archive	Manual Download	None
8. bounces	Bounce Logs	Manual Download	None
9. cli_logs	CLI Audit Logs	Manual Download	None
10. cloud_connector	Cloud Connector Logs	Manual Download	None

11. content_scanner	Content Scanner Logs	Manual Download	None
12. csa	Cisco Security Awareness Logs	Manual Download	None
13. csn_logs	CSN Logs	Manual Download	None
14. ctr_logs	CTR Logs	Manual Download	None
15. dlp	DLP Logs	Manual Download	None
16. eaas	Advanced Phishing Protection Logs	Manual Download	None
17. ecs	ESA Cloud Scanner Logs	Manual Download	None
18. encryption	Encryption Logs	Manual Download	None
19. error_logs	IronPort Text Mail Logs	Manual Download	None
20. euq_logs	Spam Quarantine Logs	Manual Download	None
21. euqgui_logs	Spam Quarantine GUI Logs	Manual Download	None
22. ftpd_logs	FTP Server Logs	Manual Download	None
23. gmarchive	Graymail Archive	Manual Download	None
24. graymail	Graymail Engine Logs	Manual Download	None
25. gui_logs	HTTP Logs	Manual Download	None
26. ipr_client	IP Reputation Logs	Manual Download	None
27. mail_logs	IronPort Text Mail Logs	Manual Download	None
28. remediation	Remediation Logs	Manual Download	None
29. reportd_logs	Reporting Logs	Manual Download	None
30. reportqueryd_logs	Reporting Query Logs	Manual Download	None
31. s3_client	S3 Client Logs	Manual Download	None
32. scanning	Scanning Logs	Manual Download	None
33. sdr_client	Sender Domain Reputation Logs	Manual Download	None
34. service_logs	Service Logs	Manual Download	None
35. slbld_logs	Safe/Block Lists Logs	Manual Download	None
36. smartlicense	Smartlicense Logs	Manual Download	None
37. snmp_logs	SNMP Logs	Manual Download	None
38. sntpd_logs	NTP logs	Manual Download	None
39. status	Status Logs	Manual Download	None
40. system_logs	System Logs	Manual Download	None
41. threatfeeds	Threat Feeds Logs	Manual Download	None
42. trackerd_logs	Tracking Logs	Manual Download	None
43. updater_logs	Updater Logs	Manual Download	None
44. upgrade_logs	Upgrade Logs	Manual Download	None
45. url_rep_client	URL Reputation Logs	Manual Download	None

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.
- CEFLOGHEADERS - Configure list of headers to add in CEF log files.
- HOSTKEYCONFIG - Configure SSH host keys.

[> **ceflogheaders**

Enter the list of headers to add in the CEF log files.

You can add multiple headers separated by commas.

[> mail-id, mail-id1, mail-id, mail-id2

rollovernow

Description

Roll over a log file.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

```
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. "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
24. All Logs
Which log would you like to roll over?
[]> 2
Log files successfully rolled over.
mail3.example.com>
```

snmpconfig

Description

Configure SNMP.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In the following example, the snmpconfig command is used to enable SNMP on the "PublicNet" interface on port 161. A passphrase for version 3 is entered and then re-entered for confirmation. The system is configured to service version 1 and 2 requests, and the community string public is entered for GET requests from those versions 1 and 2. The trap target of snmp-monitor.example.com is entered. Finally, system location and contact information is entered.

```
mail1.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? [Y]>
SNMP default version is V3

Choose an IP interface for SNMP requests.
1. Management (10.10.4.5/27: mail1.example.com) [1]>

Which port shall the SNMP daemon listen on?
[161]>

Select SNMPv3 security level:
1. noAuthNoPriv - Authentication is done using the SNMPv3 username, and no privacy is
   activated.
2. authNoPriv - Authentication is done using the SNMPv3 authentication passphrase, and no
   privacy is activated.
3. authPriv - Authentication is done using the SNMPv3 authentication passphrase, and privacy
   is activated using the SNMPv3 privacy passphrase.
[3]>

Select SNMPv3 authentication type:
1. SHA
[1]>

Select SNMPv3 privacy protocol:
1. AES
[1]>

Enter the SNMPv3 authentication passphrase.
[]>

The SNMPv3 passphrase must be at least 8 characters.

Enter the SNMPv3 authentication passphrase.
[]>

Enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Enter the SNMPv3 privacy passphrase again to confirm.
[]>
Warning: The same authentication and privacy passwords reduce the security of the system.

Do you want to set other passwords? [Y]> n

Service SNMP V1/V2c requests? [N]> Y

Enter the SNMP V1/V2c community string.
[ironport]>

Shall SNMP V2c requests be serviced from IPv4 addresses? [Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate multiple networks
with commas.
```

```
[127.0.0.1/32]>

Select the version for SNMP traps:
1. 2c
2. 3
[2]>

Enter the Trap target as a host name, IP address or list of IP addresses separated by commas
(IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 10.10.0.28

Enterprise Trap Status
1. CPUUtilizationExceeded Disabled
2. FIPSMODEDisableFailure Enabled
3. FIPSMODEEnableFailure Enabled
4. FailoverHealthy Enabled
5. FailoverUnhealthy Enabled
6. connectivityFailure Disabled
7. keyExpiration Enabled
8. linkUpDown Enabled
9. memoryUtilizationExceeded Disabled
10. resourceConservationMode Enabled
11. updateFailure Enabled

Do you want to change any of these settings? [N]>

Enter the System Location string.
[Unknown: Not Yet Configured]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.10.4.5/27 port 161.
SNMP v3: Enabled.
Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32,fe::1/64.
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target: 10.10.0.28
Location: Unknown: Not Yet Configured
System Contact: snmp@localhost

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
mail1.example.com > commit
```

tail

Description

Continuously display the end of a log file. The tail command also accepts the name or number of a log to view as a parameter: tail 9 or tail mail_logs.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

Batch Command: This command does not support a batch format.

Example

```
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>
```

Reporting

This section contains the following CLI commands:

reportingconfig

Using the reportingconfig command

The following subcommands are available within the reportingconfig submenu:

Table 12: reportingconfig Subcommands

Syntax	Description	Availability
filters	Configure filters for the Cisco Secure Email Gateway.	M-Series only
alert_timeout	Configure when you will be alerted due to failing to get reporting data.	M-Series only
domain	Configure domain report settings.	M-Series only
mode	Enable centralized reporting on the Cisco Secure Email Gateway. Enable centralized or local reporting for the email gateway.	C-, M-Series
mailsetup	Configure reporting for the email gateway.	C-Series only

Usage

Commit: This command requires a 'commit'.

Example: Enabling Reporting Filters (M-Series only)

```
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.
[]>
```

Enabling HAT REJECT Information for Domain Reports (M-Series only)

```
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.
[]>
```

Enabling Timeout Alerts (M-Series only)

```
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.
[]>
```

Enabling Centralized Reporting for an Email Gateway

```
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.
[]>
```

Configure Storage Limit for Reporting Data (C-Series only)

```
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.
[>

```

Improving Phishing Detection using Service Logs

This section contains the following CLI command:

- [servicelogsconfig](#), on page 278

servicelogsconfig

- [Description](#), on page 279
- [Usage](#), on page 279
- [Example - Enabling Service Logs on Email Gateway](#), on page 279
- [Example - Disabling Service Logs on Email Gateway](#), on page 279

Description

The `servicelogsconfig` command is used to enable or disable Service Logs on your email gateway.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Example - Enabling Service Logs on Email Gateway

In the following example, you can use the `servicelogsconfig` command to enable Service Logs on your email gateway.

```
mail1.example.com> servicelogsconfig

Share limited data with Service Logs Information Service: Disabled.

Choose the operation you want to perform:
- SETUP - Configure Service Logs settings
[]> setup

Do you want to share data with the Service Logs Information Service (recommended)? [N]>
yes

Share limited data with Service Logs Information Service: Enabled

Choose the operation you want to perform:
- SETUP - Configure Service Logs settings
[]>
```

Example - Disabling Service Logs on Email Gateway

In the following example, you can use the `servicelogsconfig` command to disable Service Logs on your email gateway.

```
mail1.example.com> servicelogsconfig

Share limited data with Service Logs Information Service: Enabled.

Choose the operation you want to perform:
- SETUP - Configure Service Logs settings
[]> setup

Do you want to share data with the Service Logs Information Service (recommended)? [N]>
no

The system will no longer share data with Service Logs.
Are you sure you want to disable (not recommended)? [N]> yes

Share limited data with Service Logs Information Service: Disabled

Choose the operation you want to perform:
- SETUP - Configure Service Logs settings
[]>
```

Sender Domain Reputation Filtering

This section contains the following CLI commands:

- [sdrconfig](#), on page 280
- [sdradvancedconfig](#), on page 282
- [sdrdiagnostics](#), on page 282

sdrconfig

- [Description](#), on page 280
- [Usage](#), on page 280
- [Example](#), on page 280
- [Example – Blocking Messages based on SDR Verdicts at SMTP Conversation Level](#), on page 281

Description

The `sdrconfig` command is used to enable SDR filtering on your email gateway.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: `help sdrconfig`.

Example

In the following example, you can use the `sdrconfig` command to enable SDR filtering on your email gateway.

```
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**

Example – Blocking Messages based on SDR Verdicts at SMTP Conversation Level

In the following example, you can use the `sdrconfig` command to block messages based on the SDR verdicts (for example, 'Untrusted,' 'Questionable,' and 'Unknown') at the SMTP conversation level.

```
mail.example.com > sdrconfig

Would you like to disable the Sender Domain Reputation check? [N]> no

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]>

Do you want to block messages based on Sender Domain Reputation threat level? [Y]> yes

Threat levels configured to be blocked currently:
"Untrusted"

Sender Domain Reputation Threat Levels:
1. Untrusted
2. Questionable
3. Neutral
4. Favorable
Choose the sender domain reputation threat level upto which email should be blocked. Enter 0 to select none of the threat levels:[1]> 2

Do you want to block messages for threat level Unknown verdict? [N]> yes

Email with the following Sender Domain Reputation threat levels will be blocked:
"Untrusted Questionable Unknown"

NOTE: Email with the Sender Domain Reputation threat level as 'Trusted' will always be allowed.
```

```
mail1.example.com> commit

Please enter some comments describing your changes:
[ ]> Changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Nov 23 09:46:31 2021 GMT
mail1.example.com>
```

sdradvancedconfig

- [Description, on page 282](#)
- [Usage, on page 282](#)
- [Example, on page 282](#)

Description

The `sdradvancedconfig` command is used to configure advanced parameters when connecting your email gateway to the SDR service.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. For more details, see the inline help by typing the command: `help sdradvancedconfig`.

Example

In the following example, you can use the `sdradvancedconfig` command to configure advanced parameters when connecting your email gateway to the SDR service.

```
mail.example.com > sdradvancedconfig

Enter SDR query timeout in seconds [5]> 3

Do you want exception list matches based on envelope-from domain only? [Y]>
```

sdrdiagnostics

- [Description, on page 283](#)
- [Usage, on page 283](#)
- [Example, on page 283](#)

Description

The `sdrdiagnostics` command is used to check if your email gateway is connected to the SDR service.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to the machine mode.

Batch Command: This command does not support a batch format.

Example

In the following example, you can use the `sdrdiagnostics` command to check if your email gateway is connected to the SDR service.

```
mail.example.com > sdrdiagnostics

1. Show status of the domain reputation service
[1]> 1
Connection Status: Connected
```

Mailbox Auto Remediation

This section contains the following CLI commands:

- [marstatus](#), on page 283
- [marupdate](#), on page 284

marstatus

- [Description](#), on page 283
- [Usage](#), on page 283
- [Example](#), on page 283

Description

The `marstatus` command is used to display the current version of the MAR component.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to the machine mode.

Batch Command: This command does not support a batch format.

Example

In the following example, you can use the `marstatus` command to view the current version of the Mailbox Auto Remediation component.

```
mail.example.com> marstatus

Component                Version                Last Updated
Mailbox Remediation      1.0                   29 Jun 2019 04:22 (GMT +00:00)
```

marupdate

- [Description, on page 284](#)
- [Usage, on page 284](#)
- [Example, on page 284](#)

Description

The `marupdate` command is used to manually update the MAR component.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to the machine mode.

Batch Command: This command does not support a batch format.

Example

In the following example, you can use the `marupdate` command to manually update the Mailbox Auto Remediation component.

```
mail.example.com > marupdate

Requesting update of Mailbox Remediation component.
```

Smart Software Licensing

This section contains the following CLI commands:

- [license_smart, on page 284](#)
- [show_license, on page 294](#)
- [smartaccountinfo, on page 295](#)

license_smart

- [Description, on page 285](#)
- [Usage, on page 285](#)
- [Example: Configuring Port for Smart Agent Service, on page 285](#)
- [Example: Enabling Smart Licensing, on page 285](#)

- [Example: Registering the Email Gateway with the Smart Software Manager, on page 286](#)
- [Example: Status of Smart Licensing, on page 286](#)
- [Example: Status Summary of Smart Licensing, on page 287](#)
- [Example: Setting the Smart Transport URL, on page 287](#)
- [Example: Requesting Licenses, on page 287](#)
- [Example: Releasing Licenses, on page 288](#)
- [Example - Enabling Smart Software Licensing for all Machines in Cluster , on page 288](#)
- [Example - Registering all Machines in Cluster with Cisco Smart Software Manager , on page 289](#)
- [Example - Enabling and Registering License Reservation, on page 289](#)
- [Example - Updating License Reservation, on page 291](#)
- [Example - Removing License Reservation, on page 291](#)
- [Example - Disabling License Reservation, on page 292](#)
- [Example - Enabling License Reservation in Cluster Mode, on page 293](#)
- [Example - Disabling License Reservation in Cluster Mode, on page 293](#)
- [Example - Enabling Device Led Conversion Process Manually, on page 294](#)

Description

Configure smart software licensing feature.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used only in machine mode. This command does not support cluster and group mode.

Batch Command: This command supports a batch format. For details, see the inline help by typing the command: `help license_smart`

Example: Configuring Port for Smart Agent Service

```
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]>
```

Example: Enabling Smart Licensing

```
mail.example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
```

Example: Registering the Email Gateway with the Smart Software Manager

```

[ ]> 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]>

```

Example: Registering the Email Gateway with the Smart Software Manager

```

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
8WlpCQ1lMbGVMQWRxOXhuenN4OWZDdktFckJLQzF5V3VIbzkYTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
registration.

```

Example: Status of Smart Licensing

```

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)

```

Example: Status Summary of Smart Licensing

```
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
```

Example: Setting the Smart Transport URL

```
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.
```

Example: Requesting Licenses



Note Users of virtual email gateway must register their email gateway to request for or release the licenses.

```
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
```

Example: Releasing Licenses

```

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.

```

Example: Releasing Licenses

```

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
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:
[ ]>

```

Example - Enabling Smart Software Licensing for all Machines in Cluster

In this example, you can use the `license_smart > enable` sub command to enable smart software licensing for all the machines in the cluster.

```
(Machine mail1.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.
[ ]> 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 if none of the features are available 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 available in the Classic Licensing mode will be available in the Evaluation period.

```
Do you want to enable Smart Software Licensing for all machines in cluster[Y/N]? [ ]> yes
```

```

Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
[Y/N] []> yes

Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]>
(Machine maill.example.com)> commit
Please enter some comments describing your changes:
[]>
Changes committed: Mon Jan 04 14:10:26 2021 GMT
(Machine maill.example.com)>

```

Example - Registering all Machines in Cluster with Cisco Smart Software Manager

In this example, you can use the `license_smart>register` sub command to register all the machines in the cluster with Cisco Smart Software Manager.

```
(Machine maill.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]> y
```

```

Enter token to register the product:
[]> YTFmZWtMtOTU.....

```

```
Do you want to register Smart Software Licensing across machines in cluster[Y/N]? []> yes
```

```

The registration is in progress for the following machines:
maill.example.com

```

```

You need to switch to the machine mode to view the Smart Software Licensing details for the
particular machine.
(Machine maill.example.com)>

```

Example - Enabling and Registering License Reservation

In this example, you can use the `license_smart>enable_reservation` sub command to enable and register the license reservation in your email gateway.

```
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.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your email

```

Example - Enabling and Registering License Reservation

```

gateway.
[> enable_reservation

Would you like to reserve license, then type "Y" else type "N" [Y/N] [> yes

License Reservation is enabled for the following machines:
maill.example.com

License Reservation is enabled

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email
gateway.
- REQUEST_CODE - Provide the request code generated on your email gateway.
[> request_code

The generation of the request code is initiated...

Copy the request code obtained on your email gateway and paste it in the Cisco Smart Software
Manager portal to select the required license

Request code: CD-ZESA:BD20B624E904-B7HCL9scQ-DD

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email
gateway.
- REQUEST_CODE - Provide the request code generated on your email gateway.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your email gateway.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your email gateway.
[> install_authorization_code
1. Paste via CLI
2. Import the Authorization Code from a file

How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>7b654af6-9d60-46f5-a79-.....PS/o+6</signature><udi>P:ESA,
S:BE30B124E904</udi></specificPLR>
^D
The SPECIFIC license reservation is successfully installed on your email gateway
Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email
gateway.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your email gateway.
- CONFIRM_CODE - Provide the confirmation code generated on your email gateway.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your email
gateway.
[>

```


Example - Updating License Reservation

In this example, you can use the `license_smart > reauthorize` sub command to reserve license for a new feature or modify the existing license reservation for a feature.

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email gateway.
- REAUTHORIZE - Install the authorization code to update specific or permanent license reservations on your email gateway.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure email gateway.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your email gateway.

```
[ ]> reauthorize
```

```
1. Paste via CLI
```

```
2. Import the Authorization Code from a file
```

```
How would you like to install Authorization Code?
```

```
[1]>
```

```
Paste the Authorization code now.
```

```
Press CTRL-D on a blank line when done.
```

```
<specificPLR><authorizationCode><flag>A</flag><version>
C</version><piid>6b684af8-4d20-42f5-ab89-.....</authorizationCode>
<signature>MEYCIDS7IZQuLvMMmiXMH2eZOWf7cy6rjgc7kxBIja</signature><udi>P:ESA,
S:BD660B174E904</udi></specificPLR>
^D
```

The SPECIFIC license reservation is successfully installed on your email gateway.

Copy the confirmation code obtained from Smart Agent and add it to the Cisco Smart Software Manager portal to update the specific reservation.

```
Confirmation code: 1f87b235
```

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email gateway.
- REAUTHORIZE - Install the authorization code to update specific or permanent license reservations on your email gateway.
- CONFIRM_CODE - Provide the confirmation code generated on your email gateway.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your email gateway.

```
[ ]>
```

Example - Removing License Reservation

In this example, you can use the `license_smart > return_reservation` sub command to remove the specific or permanent license reservation for the features enabled in your email gateway.

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email gateway.
- REAUTHORIZE - Install the authorization code to update specific or permanent license

Example - Disabling License Reservation

```

reservations on your email gateway.
- CONFIRM_CODE - Provide the confirmation code generated on your email gateway.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your email
gateway.
[> return_reservation

```

After you return the license reservation, you cannot use any of the product features, if the evaluation period has exceeded 90 days. After the 90 days evaluation period, you must register your product with Cisco Smart Software Manager to continue to use the product features. [N]> **yes**

The generation of the return code is initiated...

Copy the return code obtained on your email gateway and paste it in the Cisco Smart Software Manager portal.

```
Return Code: C97xKY-otSY8D-ertAf-v-fbEu5q-APo
```

```

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email
gateway.
- REQUEST_CODE - Provide the request code generated on your email gateway.
[>

```

```
mail1.example.com>
```

Example - Disabling License Reservation

In this example, you can use the `license_smart > disable_reservation` sub command to disable the license reservation on your email gateway.

```
mail.example.com > license_smart
```

```

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your email
gateway.
- REQUEST_CODE - Provide the request code generated on your email gateway.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your email gateway.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your email gateway.
[> disable_reservation

```

A request code for the specific or permanent reservation is generated on your email gateway. If you want to disable the reservation, it cancels the request code.

```
Do you want to disable the specific or permanent reservation? [Y/N] [ ]> yes
```

```
License Reservation is disabled for the following machines:
mail1.example.com
```

```
License Reservation is disabled
```

```

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.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your email gateway.
[]>
```

Example - Enabling License Reservation in Cluster Mode

In this example, you can use the `license_smart > enable_reservation` sub command to enable the license reservation for all machines in the cluster.

```
(Machine mail1.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.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Email Gateway.
[]> enable_reservation
```

```
Would you like to reserve license, then type "Y" else type "N" [Y/N] []> yes
```

```
Do you want to enable License Reservation for all machines in cluster[Y/N]? []> yes
```

```
License Reservation is enabled for the following machines:
mail1.example.com, mail2.example.com
```

```
Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Email Gateway.
- REQUEST_CODE - Provide the request code generated on your Email Gateway.
[]>
```

Example - Disabling License Reservation in Cluster Mode

In this example, you can use the `license_smart > disable_reservation` sub command to disable the license reservation for all machines in the cluster.

```
Machine mail1.example.com)> license_smart
```

```
Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Email Gateway.
- REQUEST_CODE - Provide the request code generated on your Email Gateway.
[]> disable_reservation
```

```
Do you want to disable License Reservation for all machines in cluster[Y/N]? []> yes
```

```
License Reservation is disabled for the following machines:
```

```
mail1.example.com, mail2.example.com
```

To start using the licenses, please register the product.

```
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
```

Example - Enabling Device Led Conversion Process Manually

```

- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Email Gateway.
[]>

```

Example - Enabling Device Led Conversion Process Manually

In this example, you can use the `license_smart > conversion_start` sub command to enable the Device Led Conversion (DLC) process manually on your email gateway.

```
mail.example.com > license_smart
```

Deregister your email gateway from the Cisco Smart Software Manager portal to enable the license reservation

Choose the operation you want to perform:

```

- URL - Set the Smart Transport URL.
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- DEREGISTER - Deregister the product from Smart Licensing.
- REREGISTER - Reregister the product for Smart Licensing.
- RENEW_AUTH - Renew authorization of Smart Licenses in use.
- RENEW_ID - Renew registration with Smart Licensing.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- CONVERSION_START - To manually convert the classic license keys to smart Licensing
[]> conversion_start

```

Do you want to start the process of converting your classic license keys to smart software licensing[Y/N]? []> **yes**

show_license

- [Description, on page 294](#)
- [Example: Status of Smart Licensing, on page 294](#)
- [Example: Status Summary of Smart Licensing, on page 295](#)

Description

Show Smart Licensing status and summary of status.

Example: Status of Smart Licensing

```

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)
```

Example: Status Summary of Smart Licensing

```
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
```

smartaccountinfo

- [Description, on page 295](#)
- [Usage, on page 295](#)
- [Example: Viewing Smart Account Details, on page 295](#)

Description

The `smartaccountinfo` command is used to view details of the smart account created in the Cisco Smart Software Manager portal

Usage

Commit: This command requires a 'commit.'

Cluster Management: This command can be used in all three machine modes (cluster, group, and machine).

Batch Command: This command supports a batch format.

Example: Viewing Smart Account Details

In this example, you can use the `smartaccountinfo` command to view details of the smart account created in the Cisco Smart Software Manager portal:

```
mail1.example.com> smartaccountinfo

Smart Account details
-----

Product Instance ID: b56r42423-5sdf-5fsf-7823-r24gf32ad334s
Smart Account Domain: exampleaccount.cisco.com
Smart Account ID: 111111
Smart Account Name : exampleaccount.cisco.com
VLN: VLNES111111
Virtual Account Domain: ESA
Virtual Account ID: 333333
mail1.example.com>
```

SMTP Services Configuration

This section contains the following CLI commands:

callaheadconfig

Description

Add, edit, and remove SMTP Call-Ahead profiles

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In the following example you can create a new SMTP call-ahead profile for delivery host.

```
> 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
  TLS support for recipient validation: disabled
  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.
[ ]>
```

In the following example you can create a new SMTP call-ahead profile for call ahead server.

```
> 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
TLS support for recipient validation: disabled
  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]>
```

Example – Enabling TLS Support for SMTP Call-ahead Recipient Validation

In the following example, you can use the `callaheadconfig` command to enable TLS support for recipient validation in an existing SMTP call-ahead profile.

```
mail1.example.com> callaheadconfig

Currently configured SMTP Call-Ahead profiles:
1. call-ahead-1 (Static Call-Ahead Servers)
2. call-ahead-2 (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.
```

Example – Enabling TLS Support for SMTP Call-ahead Recipient Validation

```

- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[ ]> edit

Select the profile you want to edit:
1. call-ahead-1 (Static Call-Ahead Servers)
2. call-ahead-2 (Delivery Host)
[1]> 1

Please enter a name for the profile:
[call-ahead-1]>

Select the type of profile you want to create:
1. Delivery Host
2. Static Call-Ahead Servers
[2]>

Enter one or more Call-Ahead servers hostname separated by commas.
[[10.12.2.40]:25]>

Advanced Settings:
MAIL FROM Address: <>
Interface: Auto
TLS support for recipient validation: disabled
Timeout Value: 30
Validation Failure Action: Reject
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]> yes

TLS support for SMTP call-ahead recipient validation is: disabled

Do you want to enable TLS support for SMTP call-ahead recipient
validation? y/n [Y]> yes

Enter MAIL FROM address (Enter NONE to set it to blank string)
[ ]>

Please choose an IP interface for this profile:
1. Auto
2. Management (10.12.2.3/24: mail1.example.com)
[1]>

Specify the validation request timeout (in seconds):
[30]>

Specify the default action for non-verifiable recipients:
1. REJECT
2. REJECT with custom code
3. ACCEPT
[1]>

Specify the default action for temporary failure (4xx error):
1. REJECT with same code
2. REJECT with custom code
3. ACCEPT
[1]>

Enter maximum number of recipients to validate per SMTP session:
[1000]>

```



```

Enter maximum number of simultaneous
connections to Call-Ahead server:
[5]>

Enter cache entries:
[10000]>

Enter cache TTL (in seconds):
[900]>

Currently configured SMTP Call-Ahead profiles:
1. call-ahead-1 (Static Call-Ahead Servers)
2. call-ahead-2 (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.
[ ]>

mail1.example.com> commit

Please enter some comments describing your changes:
[ ]> changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Mon June 21 18:37:42 2021 GMT
mail1.example.com>

```

listenerconfig

Description

The `listenerconfig` command allows you to create, edit, and delete a listener. AsyncOS requires that you specify criteria that messages must meet in order to be accepted and then relayed to recipient hosts — either internal to your network or to external recipients on the Internet.

These qualifying criteria are defined in listeners; collectively, they define and enforce your mail flow policies. Listeners also define how the email gateway communicates with the system that is injecting email.

Table 13: listenerconfig Commands

Name	Unique nickname you supply for the listener, for future reference. The names you define for listeners are case-sensitive. AsyncOS does not allow you to create two identical listener names.
IP Interface	Listeners are assigned to IP interfaces. All IP interfaces must be configured using the <code>systemstartup</code> command or the <code>interfaceconfig</code> command before you create and assign a listener to it.
Mail protocol	The mail protocol is used for email receiving: either ESMTP or QMQP

IP Port	The specific IP port used for connections to the listener. by default SMTP uses port 25 and QMQP uses port 628.
Listener Type: Public Private Sink hole	Public and private listeners are used for most configurations. By convention, private listeners are intended to be used for private (internal) networks, while public listeners contain default characteristics for receiving email from the Internet. “Sink hole” listeners can be used for testing or troubleshooting purposes. When you create a sink hole listener, you choose whether messages are written to disk or not before they are deleted. (See the “Testing and Troubleshooting” chapter of the <i>User Guide for AsyncOS for Cisco Secure Email Gateway</i> for more information.)

Usage

Commit: This command requires a ‘commit’.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format - General listenerconfig

The batch format of the **listenerconfig** command can be used to add and delete listeners on a particular interface. The batch format of the listenerconfig command also allows you to configure a listener’s HAT and RAT.

- Adding a new listener:

```
listenerconfig new <name> <public|private|sinkhole|sinkholequeueing>
<interface_name> <smtp|qmqp>
```

- Deleting a listener:

```
listenerconfig delete <name>
```

Batch Format - HAT

The following examples demonstrate the use of the batch format of listenerconfig to perform various HAT-related tasks. For more information about arguments, consult *Table - listenerconfig Argument Values -HAT* below:

- Adding a new sendergroup to the HAT

```
listenerconfig edit <name> hostaccess new sendergroup <name> <host_list> <behavior>
[options [--comments]
```

- Add a new policy to the HAT

```
listenerconfig edit <name> hostaccess new policy <name> <behavior> [options]
```

- Add a new host list to a sendergroup

```
listenerconfig edit <name> hostaccess edit sendergroup <name> new <host_list>
```

- Delete a host from a sendergroup

```
listenerconfig edit <name> hostaccess edit sendergroup <name> delete <host>
```

- Move a host in a sendergroup's list order

```
listenerconfig edit <name> hostaccess edit sendergroup <name> move <host>  
<host-to-insert-before>
```

- Modify a sendergroup's policy

```
listenerconfig edit <name> hostaccess edit sendergroup <name> policy <behavior> [options]
```

- Print a sendergroup listing

```
listenerconfig edit <name> hostaccess edit sendergroup <name> print
```

- Rename a sendergroup

```
listenerconfig edit <name> hostaccess edit sendergroup <name> rename <name>
```

- Editing a HAT's policy

```
listenerconfig edit <name> hostaccess edit policy <name> <behavior> [options]
```

- Deleting a sendergroup from a HAT

```
listenerconfig edit <name> hostaccess delete sendergroup <name>
```

- Deleting a policy

```
listenerconfig edit <name> hostaccess delete policy <name>
```

- Moving a sendergroup's position in the HAT

```
listenerconfig edit <name> hostaccess move <group> <group-to-insert-before>
```

- Changing a HAT default option

```
listenerconfig edit <name> hostaccess default [options]
```

- Printing the hostaccess table

```
listenerconfig edit <name> hostaccess print
```

- Import a local copy of a HAT

```
listenerconfig edit <name> hostaccess import <filename>
```

- Exporting a copy of the HAT from the email gateway

```
listenerconfig edit <name> hostaccess export <filename>
```

- Deleting all user defined sendergroups and policies from the HAT

```
listenerconfig edit <name> hostaccess clear
```

- Adding the sender's country of origin for a particular sender group.

```
listenerconfig edit incoming hostaccess edit sendergroup ALLOWED_LIST
country add India Nepal Cyprus
```

- Deleting the sender's country of origin for a particular sender group.

```
listenerconfig edit incoming hostaccess edit sendergroup ALLOWED_LIST
country delete Cyprus
```

- Printing the sender's country of origin for a particular sender group.

```
listenerconfig edit incoming hostaccess edit sendergroup ALLOWED_LIST
country print
```

Table 14: listenerconfig Argument Values -HAT

Argument	Description
<behavior>	“Accept”, “Relay”, “Reject”, “TCP Refuse”, or “Continue”. When selecting a behavior for use with a sendergroup, additional behaviors of the form “Policy: FOO” are available (where “FOO” is the name of policy).
<filename>	The filename to use with importing and exporting the hostaccess tables.
<group>	A sendergroup <name>.
<host>	A single entity of a <host_list>

Argument	Description
<host_list>	Enter the hosts to add. Hosts can be formatted as follows: CIDR addresses (10.1.1.0/24) IP address ranges (10.1.1.10-20) IP Subnets (10.2.3) Hostname (crm.example.com) Partial Hostname (.example.com) Sender Base Reputation Score range (7.5:10.0) Senderbase Network Owner IDS (SBO:12345) Remote blocked_list queries (dnslist[query.blocked_list.example]) Note Separate multiple hosts with commas
<name>	The name of the sendergroup or policy. HAT labels must start with a letter or underscore, followed by any number of letters, numbers, underscores or hyphens.
[options]	
--max_size	Maximum message size. Add a trailing k for kilobytes, M for megabytes, or no letters for bytes.
--max_conn	Maximum number of connections allowed from a single host.
--max_msgs	Maximum number of messages per connection.
--max_rcpt	Maximum number of recipients per message.
--override	Override the hostname in the SMTP banner. "No" or SMTP banner string.
--cust_acc	Specify a custom SMTP acceptance response. "No" or SMTP acceptance response string.
--acc_code	Custom SMTP acceptance response code. Default is 220.
--cust_rej	Specify a custom SMTP rejection response. "No" or SMTP rejection response string.
--rej_code	Custom SMTP rejection response code. Default is 554.
--rate_lim	Enable rate limiting per host. "No", "default" or maximum number of recipients per hour per host.
--cust_lim	Specify a custom SMTP limit exceeded response message. "No" or SMTP rejection response string. Default is "No".
--lim_code	Custom SMTP limit exceeded response code. Default is 452.
--use_sb	Use SenderBase for flow control by default. "Yes", "No", or "default".
--as_scan	Enable anti-spam scanning. "Yes", "No", "Default".

Argument	Description
--av_scan	Enable anti-virus scanning. “Yes”, “No”, “Default”.
-sdr_scan	Enable Sender Domain Reputation scanning. "Yes," "No," "Default."
--dhap	Directory Harvest Attack Prevention. “No”, “default”, or maximum number of invalid recipients per hour from a remote host.
--tls	Not supported; use menuing system to configure TLS.
--sig_bits	Number of bits of IP address to treat as significant. From 0 to 32, “No” or “default”.
--dkim_signing	Enable DKIM signing. “Yes”, “No”, “Default.”
--dkim_verification	Enable DKIM verification. “Yes”, “No”, “Default.”
--dkim_verification_profile <name>	The name of DKIM verification profile. This option is only applicable if --dkim_verification value is set to “Yes.”
--spf	Enable SPF verification. “Yes”, “No”, “Default.”
--spf_conf_level	SPF conformance level. Used with “--spf Yes” only. “spf_only”, “sidf_compatible”, “sidf_strict.”
--spf_downgrade_pra	Downgrade SPF PRA verification result. Used with “--spf Yes” and “--spf_conf_level sidf_compatible” only. “Yes”, “No.”
--spf_helo_test	SPF HELO test. Used with “--spf Yes” and “--spf_conf_level sidf_compatible,” or “--spf_conf_level spf_only.” “Yes”, “No”.
--dmarc_verification	Enable DMARC verification. “Yes”, “No”, “Default.”
--dmarc_verification_profile <name>	The name of DMARC verification profile. This option is only applicable if --dmarc_verification value is set to “Yes.”
--dmarc_agg_reports	Enable DMARC aggregate reports. “Yes”, “No”, “Default.” This option is only applicable if --dmarc_verification value is set to “Yes.”

Batch Format - RAT

The following examples demonstrate the use of the batch format of listenerconfig to perform various RAT-related tasks. For more information about arguments, consult *Table - listenerconfig Argument Values - RAT* below:

- Adding a new recipient to the RAT

```
listenerconfig edit <name> rcptaccess new <rat_addr> [options]
```

- Editing a recipient in the RAT

```
listenerconfig edit <name> rcptaccess edit <rat_addr> [options]
```

- Deleting a recipient from the RAT

```
listenerconfig edit <name> rcptaccess delete <rat_addr>
```

- Printing a copy of the RAT

```
listenerconfig edit <name> rcptaccess print
```

- Importing a local RAT to your email gateway

```
listenerconfig edit <name> rcptaccess import <filename>
```

- Exporting a RAT

```
listenerconfig edit <name> rcptaccess export <filename>
```

- Clearing the default access

```
listenerconfig edit <name> rcptaccess clear <default_access>
```

Table 15: listenerconfig Argument Values - RAT

Argument	Description
<rat_addr>	Enter the hosts to add. Hosts can be formatted as follows: CIDR addresses (10.1.1.0/24) Hostname (crm.example.com) Partial Hostname (.example.com) Usernames (postmaster@) Full email addresses (joe@example.com, joe@[1.2.3.4]) Note Separate multiple hosts with commas
<options>	
--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 query. Either "Yes" or "No."
--bypass_ca	Bypass SMTP Call-Ahead. Default is "No".

Example - Adding a listener

In the following example, the `listenerconfig` command is used to create a new private listener called `OutboundMail` that can be used for the B listener needed in the Enterprise Gateway configuration. (Note: you also had the option to add this private listener during the GUI's System Setup Wizard CLI `systemsetup` command.)

A private listener type is chosen and named `OutboundMail`. It is specified to run on the `PrivateNet` IP interface, using the SMTP protocol over port 25. The default values for the Host Access Policy for this listener are then accepted.

```
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.
[ ]> new
Please select the type of listener you want to create.
1. Private
2. Public
3. Sinkhole
[2]> 1
Please create a name for this listener (Ex: "OutboundMail"):
[ ]> 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.
[ ]> .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.
[]>
```

Example - Adding a Sender's Country of Origin to a Sender Group

In the following example, the listenerconfig command is used to modify a listener to add the sender's country of origin for a particular sender group.

```
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
```

Example - Adding a Sender's Country of Origin to a Sender Group

```
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. ALLOWED_LIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLOCKED_LIST (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.
```

Example - Adding a Sender's Country of Origin to a Sender Group

```
- 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]
```

Example - Customizing the Host Access Table (HAT) for a listener via Export and Import

Many of the subcommands within the listenerconfig command allow you to import and export data in order to make large configuration changes without having to enter data piecemeal in the CLI.

These steps use the CLI to modify the Host Access Table (HAT) of a listener by exporting, modifying, and importing a file. You can also use the HAT CLI editor or the GUI to customize the HAT for a listener. For more information, see the “Configuring the Gateway to Receive Mail” and “Using Mail Flow Monitor” chapters in the *User Guide for AsyncOS for Cisco Secure Email Gateway*.

To customize a HAT for a listener you have defined via export and import:

Procedure

- Step 1** Use the hostaccess -> export subcommands of listenerconfig to export the default HAT to a file.
- In the following example, the HAT for the public listener InboundMail is printed, and then exported to a file named inbound.HAT.txt

Example:

```
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.
```

Example - Customizing the Host Access Table (HAT) for a listener via Export and Import

```

- 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
    }
ALLOWED_LIST:
    $TRUSTED (My trusted senders have no anti-spam or rate limiting)
BLOCKED_LIST:
    $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".

```

Example:

Step 2 Outside of the Command Line Interface (CLI), get the file inbound.HAT.txt .

Step 3 With a text editor, create new HAT entries in the file.

In this example, the following entries are added to the HAT above the ALL entry:

spamdomain.com	REJECT
.spamdomain.com	REJECT
251.192.1.	TCPREFUSE
169.254.10.10	RELAY

- The first two entries reject all connections from the remote hosts in the domain spamdomain.com and any subdomain of spamdomain.com .

Example - Customizing the Host Access Table (HAT) for a listener via Export and Import

- The third line refuses connections from any host with an IP address of 251.192.1. x .
- The fourth line allows the remote host with the IP address of 169.254.10.10 to use the email gateway as an SMTP relay for all of its outbound email to the Internet

Note The order that rules appear in the HAT is important. The HAT is read from top to bottom for each host that attempts to connect to the listener. If a rule matches a connecting host, the action is taken for that connection immediately. You should place all custom entries in the HAT above an ALL host definition. You can also use the HAT CLI editor or the GUI to customize the HAT for a listener. For more information, see the “Configuring the Gateway to Receive Mail” and “Using Mail Flow Monitor” chapters in the *User Guide for AsyncOS for Cisco Secure Email Gateway* .

Step 4 Save the file and place it in the configuration directory for the interface so that it can be imported. (See Appendix B, “Accessing the Email Gateway,” for more information.)

Step 5 Use the `hostaccess -> import` subcommand of `listenerconfig` to import the edited Host Access Table file.

In the following example, the edited file named `inbound.HAT.txt` is imported into the HAT for the `InboundMail` listener. The new entries are printed using the `print` subcommand.

Example:

```
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.
- 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
    }

```

Example - Customizing the Host Access Table (HAT) for a listener via Export and Import

```

        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
ALLOWED_LIST:
    $TRUSTED (My trusted senders have no anti-spam scanning or rate limiting)
BLOCKED_LIST:
    $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.
[ ]>

```

Remember to issue the commit command after you import so that the configuration change takes effect.

Example - Enabling Public Key Harvesting and S/MIME Decryption and Verification

The following example shows how to:

- Retrieve (harvest) public key from the incoming S/MIME signed messages
- Enable S/MIME decryption and verification

```
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
```

Example - Enabling Public Key Harvesting and S/MIME Decryption and Verification

```

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]>
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 - Advanced HAT Parameters

The following table defines the syntax of advanced HAT parameters. Note that for the values below which are numbers, you can add a trailing **k** to denote kilobytes or a trailing **M** to denote megabytes. Values with no letters are considered bytes. Parameters marked with an asterisk support the variable syntax shown in the following table.

Table 16: Advanced HAT Parameter Syntax

Parameter	Syntax	Values	Example Values
Maximum messages per connection	<code>max_msgs_per_session</code>	Number	1000
Maximum recipients per message	<code>max_rcpts_per_msg</code>	Number	10000 1k
Maximum message size	<code>max_message_size</code>	Number	1048576 20M
Maximum concurrent connections allowed to this listener	<code>max_concurrency</code>	Number	1000
SMTP Banner Code	<code>smtp_banner_code</code>	Number	220
SMTP Banner Text (*)	<code>smtp_banner_text</code>	String	Accepted
SMTP Reject Banner Code	<code>smtp_banner_code</code>	Number	550
SMTP Reject Banner Text (*)	<code>smtp_banner_text</code>	String	Rejected
Override SMTP Banner Hostname	<code>use_override_hostname</code>	on off default	default
	<code>override_hostname</code>	String	newhostname
Use TLS	<code>tls</code>	on off required	on
Use anti-spam scanning	<code>spam_check</code>	on off	off
Use Sophos virus scanning	<code>virus_check</code>	on off	off
Maximum Recipients per Hour	<code>max_rcpts_per_hour</code>	Number	5k
Maximum Recipients per Hour Error Code	<code>max_rcpts_per_hour_code</code>	Number	452
Maximum Recipients per Hour Text (*)	<code>max_rcpts_per_hour_text</code>	String	Too manyrecipients
Use SenderBase	<code>use_sb</code>	on off	on
Define SenderBase Reputation Score	<code>sbrs [value1 :value2]</code>	-10.0- 10.0	sbrs [-10:-7.5]

Parameter	Syntax	Values	Example Values
Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour	dhap_limit	Number	150

Adding bypass_ca Argument to listenerconfig

The following example shows how to add the `bypass_ca` argument to `listenerconfig`:

```
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".
```

Example - Configuring SPF and SIDF

When configuring the default settings for a listener's Host Access Table, you can choose the listener's SPF/SIDF conformance level and the SMTP actions (ACCEPT or REJECT) that the email gateway performs, based on the SPF/SIDF verification results. You can also define the SMTP response that the email gateway sends when it rejects a message.

Depending on the conformance level, the appliance performs a check against the HELO identity, MAIL FROM identity, or PRA identity. You can specify whether the email gateway proceeds with the session (ACCEPT) or terminates the session (REJECT) for each of the following SPF/SIDF verification results for each identity check:

- **None.** No verification can be performed due to the lack of information.
- **Neutral.** The domain owner does not assert whether the client is authorized to use the given identity.
- **SoftFail.** The domain owner believes the host is not authorized to use the given identity but is not willing to make a definitive statement.
- **Fail.** The client is not authorized to send mail with the given identity.

- **TempError**. A transient error occurred during verification.
- **PermError**. A permanent error occurred during verification.

The email gateway accepts the message for a Pass result unless you configure the SIDF Compatible conformance level to downgrade a Pass result of the PRA identity to None if there are Resent-Sender: or Resent-From: headers present in the message. The email gateway then takes the SMTP action specified for when the PRA check returns None.

If you choose not to define the SMTP actions for an identity check, the email gateway automatically accepts all verification results, including Fail.

The email gateway terminates the session if the identity verification result matches a REJECT action for any of the enabled identity checks. For example, an administrator configures a listener to accept messages based on all HELO identity check results, including Fail, but also configures it to reject messages for a Fail result from the MAIL FROM identity check. If a message fails the HELO identity check, the session proceeds because the email gateway accepts that result. If the message then fails the MAIL FROM identity check, the listener terminates the session and then returns the SMTP response for the REJECT action.

The SMTP response is a code number and message that the email gateway returns when it rejects a message based on the SPF/SIDF verification result. The TempError result returns a different SMTP response from the other verification results. For TempError, the default response code is 451 and the default message text is #4.4.3 Temporary error occurred during SPF verification . For all other verification results, the default response code is 550 and the default message text is #5.7.1 SPF unauthorized mail is prohibited . You can specify your own response code and message text for TempError and the other verification results.

Optionally, you can configure the email gateway to return a third-party response from the SPF publisher domain if the REJECT action is taken for Neutral, SoftFail, or Fail verification result. By default, the email gateway returns the following response:

```
550-#5.7.1 SPF unauthorized mail is prohibited.
```

```
550-The domain example.com explains:
```

```
550 <Response text from SPF domain publisher>
```

To enable these SPF/SIDF settings, use the `listenerconfig -> edit` subcommand and select a listener. 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
```

The following SPF control settings are available for the Host Access Table:

Table 17: SPF Control Settings

Conformance Level	Available SPF Control Settings
SPF Only	<ul style="list-style-type: none"> • whether to perform HELO identity check • SMTP actions taken based on the results of the following identity checks: <ul style="list-style-type: none"> • HELO identity (if enabled) • MAIL FROM Identity • SMTP response code and text returned for the REJECT action • verification time out (in seconds)
SIDF Compatible	<ul style="list-style-type: none"> • whether to perform a HELO identity check • whether the verification downgrades a Pass result of the PRA identity to None if the Resent-Sender: or Resent-From: headers are present in the message • SMTP actions taken based on the results of the following identity checks: <ul style="list-style-type: none"> • HELO identity (if enabled) • MAIL FROM Identity • PRA Identity • SMTP response code and text returned for the REJECT action • verification timeout (in seconds)
SIDF Strict	<ul style="list-style-type: none"> • SMTP actions taken based on the results of the following identity checks: <ul style="list-style-type: none"> • MAIL FROM Identity • PRA Identity • SMTP response code and text returned in case of SPF REJECT action • verification timeout (in seconds)

The following example shows a user configuring the SPF/SIDF verification using the SPF Only conformance level. The email gateway performs the HELO identity check and accepts the None and Neutral verification results and rejects the others. The CLI prompts for the SMTP actions are the same for all identity types. The user does not define the SMTP actions for the MAIL FROM identity. The email gateway automatically accepts all verification results for the identity. The email gateway uses the default reject code and text for all REJECT results.

Example: SPF/SIDF Settings

```

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

```

Example: SPF/SIDF in Default Policy Parameters

```
[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]>
```

The following shows how the SPF/SIDF settings are displayed for the listener's Default Policy Parameters.

Example: SPF/SIDF in Default Policy Parameters

```
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
```

Example - Enable DMARC Verification

The following example shows how to enable DMARC verification.

```
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]>

```

Example - Enable DMARC Verification

```

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

Description

Configure multi-lingual settings

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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 or message body is split into separate message attachment. Do you want the
appliance 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 are found: Disclaimer or message body is added
as a message attachment.

```

```

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> mail3.example.com

```

smtpauthconfig

Description

Configure SMTP Auth outgoing and forwarding profiles.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

In the following example, the **smtpauthconfig** command is used to create a new, forwarding-based profile for the server "smtp2.example.com:"

```

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

```



Note An authenticated user is granted a RELAY HAT policy.

You may specify more than one forwarding server in a profile. SASL mechanisms CRAM-MD5 and DIGEST-MD5 are not supported between the email gateway and a forwarding server.

System Setup

systemsetup

Description

First time system setup as well as re-installation of the system.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```

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:
Would you like to get a system generated passphrase? [N]>
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

```

Example

```

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 Filtering

This section contains the following CLI commands:

aggregatorconfig

Description

Configure address for Cisco Aggregator Server on the email gateway. This server provides details of the end users who clicked on rewritten URLs and the action (allowed, blocked or unknown) associated with each user click.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

Example

```
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
```

retroscannerstatus

Description

Displays the version and update status of each updatable component used for communicating to the URL Retrospective service.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode..

Batch Command: This command does not support a batch format.

Example

In the following example, you can use the `retroscannerstatus` command to view the version and the update status of the URL Retrospective service components.

```
vm21esa0136.cs21> retroscannerstatus

Component      Version Last Updated
Cloud Retro Remediation Engine 1.0  Never updated
Cloud Retro Remediation Config 0.2  06 Apr 2022 18:00 (GMT +00:00)
Cloud Retro Client Certificate 1.0.1 06 Apr 2022 18:00 (GMT +00:00)
```

retroscannerupdate

Description

This command is used to request for an update of the URL Retrospective service engine.

Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

Example

In the following example, you can use the `retroscannerupdate` command to request for an update of the URL Retrospective service engine.

```
vm21esa0136.cs21> > retroscannerupdate
Requesting check for new Retro scanner updates
```

urllistconfig

Description

Configure or import allowed lists of URLs that will not be evaluated by URL filtering features. These lists are not used by the Outbreak Filters feature.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Example

```
> 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 allowed list.
- EDIT - Modify an existing URL allowed list.
- DELETE - Delete an existing URL allowed list.
[]>EDIT
Choose the operation to edit the URL allowed list:
- IMPORT - Import a file into an existing URL allowed list
- EXPORT - Export an existing URL allowed list into a file
- RENAME - Rename an existing URL allowed list
[]>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.
```

websecurityadvancedconfig

Description

Configure the following advanced settings for URL filtering:

- **URL Lookup Timeout:** The time taken for the URL to request the IP address for a certain domain name.
- **Maximum number of URLs to scan in message body:** The maximum number of URLs that are scanned in a message body .
- **Maximum number of URLs to scan in message attachments:** The maximum number of URLs that are scanned in the attachments of a message.
- **Rewrite URL text and HREF in the message:** You can choose whether you want the full rewritten URL to appear in the message body or the rewritten URL to only appear in the HREF for HTML messages.
- **URL logging:** Displays URL details in Mail Logs and Message Tracking.



Note Except to change timeout values for troubleshooting purposes, use this command only under the direction of Cisco support.

The timeout value is the value, in seconds, for communication with the cloud services that provide reputation and category for URLs.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format.

Batch Format

For the batch format, see the CLI inline help.

Example

```
mail.example.com> websecurityadvancedconfig
Enter URL lookup timeout in seconds:
[15]>
```

```
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]>
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]>

Logging of URLs is currently enabled.
Do you wish to disable logging of URL's? [N]>

>
```

websecurityconfig

Description

Configure basic settings for URL filtering (URL reputation and URL category features.) and mailbox remediation based on URL retrospective service.

Normally, certificate management is automatic. Unless directed to do otherwise by Cisco TAC, you should select No at the prompt to set a certificate.

Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command supports a batch format. See the inline CLI help for more details. Use the help command to access the inline help for this command.

Example

```
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 add URLs to the allowed list 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.
URL Retrospective service based Mail Auto Remediation is disabled.
URL Retrospective service status - Connected

Disable URL Filtering? [N]> N

Do you wish to disable Web Interaction Tracking? [N]> N

There are no URL lists configured currently. Create a URL list for URLs that should
be skipped by URL Filtering, using the urllistconfig command.
```

```
Enable URL Retrospective service based Mail Auto Remediation to configure remediation actions.
```

```
Do you wish to enable Mailbox Auto Remediation action? [N]> y
```

```
URL Retrospective service based Mail Auto Remediation is enabled.
```

```
Please select a Mailbox Auto Remediation action:
```

1. Delete
 2. Forward and Delete
 3. Forward
- ```
[1]> 1
```

## websecuritydiagnostics

### Description

View diagnostic statistics related to URL filtering.

### Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

### Example

```
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
```

## User Management

This section contains the following CLI commands:

### userconfig

#### Description

Manage user accounts and connections to external authentication sources.



## Usage

**Commit:** This command requires a 'commit'.

**Cluster Management:** This command is restricted to cluster mode.

**Batch Command:** This command supports a batch format. See the inline CLI help for more details. Use the help command to access the inline help for this command, for example,

```
mail.example.com> userconfig help
```

## Example - Creating a New User Account

The following example shows how to create a new user account with a Help Desk User role.

```
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.
```

## Example - Setting Up a RADIUS Server for External Authentication

```
- URLTRACKING - Configure URL tracking privileges.
[]>
```

## Example - Setting Up a RADIUS Server for External Authentication

The following example shows how to set up a RADIUS server for external authentication. To set up a RADIUS server, enter the hostname, port, shared passphrase, and whether to use CHAP or PAP for the authentication protocol.

```
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.
[]>
```

## Example - Enabling Two-Factor Authentication for Specific User Role

In the following example, the `twofactorauth` sub command is used to enable two-factor authentication for a specific user role.

```
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.
```

## Example - Enabling Two-Factor Authentication for Specific User Role

```
- 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

[]>

```

## Example – Enabling SAML Authentication

```

mail.example.com > userconfig
Users:
1. admin - "Administrator" (admin)
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.
- TWOFACORAUTH - Configure Two-Factor 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]> 10
Choose a mechanism to use:
LDAP is unavailable because no LDAP queries of type EXTERNALAUTH are configured
1. RADIUS
2. SAML
[1]> 2
Please enter the external group name to map (group names are case-sensitive):
[]> member-of
Assign a role to "member-of":
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.

```

**Example – Creating New Custom Role for AMP Configuration**

```
[1]> 1
Mapping for "member-of" to Administrators created.
Please enter group attribute to be matched in saml attributes:
[[]]> Group Name
Choose the operation you want to perform:
- SETUP - Set up global settings.
- GROUPS - Configure external group mapping.
[]> groups
There are currently 1 mappings configured.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Edit destination of an existing mapping.
- DELETE - Remove a mapping.
- CLEAR - Clear all mappings.
- PRINT - Display all mappings.
[]>
```

**Example – Creating New Custom Role for AMP Configuration**

The following example shows how to create a new custom role with AMP configuration privileges.

```
mail.example.com> > userconfig
Users:
1. admin - "Administrator" (admin)
2. ampcloud - "ampcloud" (ampcloud)
3. ampcluster - "ampcluster" (ampcluster)

Devops External authentication: Disabled
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.
[]> ROLE
User Roles:
1. AMP
2. AMP_Config - AMP_Config
3. AMP_DLP - AMP_DLP

Choose the operation you want to perform:
- NEW - Define a new role.
- EDIT - Modify an existing role.
- DELETE - Remove an existing role.
- PRINT - Display an existing role.
[]> new

Enter a name for the role.
[]> AMPConfig

Enter a short description for user role 'AMPConfig'.
[]> New role for AMP Configuration

Select type of access to mailpolicies and content filters?
1. No access
```

```

2. View assigned, edit assigned
3. View all, edit assigned
4. View all, edit all (full access)
[1]> 3

Select type of access to DLP policies?
1. No access
2. View assigned, edit assigned
3. View all, edit assigned
4. View all, edit all (full access)
[1]> 1

Select type of access to AMP Configurations?
1. No access
2. Full access
[1]> 2

Select type of access to tracking?
1. No access
2. Message Tracking access
[1]> 2

Select type of access to reports?
1. No access
2. View relevant reports
3. View all reports
[1]> 3

Select type of access to trace?
1. No access
2. Trace access
[1]> 2

Select type of access to logs?
1. No access
2. Log Subscription access
[1]> 1

Role "AMPConfig" successfully created.

```

## passphrase or passwd

### Description

Change your passphrase.

### Usage

Commit: This command requires a 'commit'.

Cluster Management: This command is restricted to cluster mode.




---

**Note** The passwd command is a special case because it needs to be usable by guest users who can only ever be in machine mode. If a guest user issues the passwd command on a machine in a cluster, it will not print the warning message but will instead just silently operate on the cluster level data without changing the user's mode. All other users will get the above written behavior (consistent with the other restricted configuration commands).

---

## Example

Batch Command: This command does not support a batch format.

## Example

```
mail3.example.com> passphrase
Old passphrase: your_old_passphrase
Would you like to get a system generated passphrase? [N]>
New passphrase: your_new_passphrase
Retype new passphrase: your_new_passphrase
passphrase changed.
```

## last

### Description

The **last** command displays who has recently logged into the system. By default, it shows all users who have logged into the system

### Usage

Commit: This command does not require a 'commit'.

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format.

## Example

```
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

### Description

The **who** command lists all users who are logged into the system via the CLI, the time of login, the idle time, and the remote host from which the user is logged in.

### Usage

Commit: This command does not require a 'commit'.



Cluster Management: This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto). This command requires access to the local file system.

**Batch Command:** This command does not support a batch format.

## Example

```
mail3.example.com> who
Username Login Time Idle Time Remote Host What
===== ===== ===== ===== =====
admin 03:27PM 0s 10.1.3.201 cli
```

## whoami

### Description

The **whoami** command displays the username and full name of the user currently logged in, and which groups the user belongs to.

### Usage

Commit: This command requires a 'commit'.

Cluster Management: This command can be used in all three machine modes (cluster, group, machine).

Batch Command: This command does not support a batch format.

## Example

```
mail3.example.com> whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

# Virtual Email Gateway Management

## loadlicense

### Description

Loads an XML license for a virtual email gateway. You can load from a file or copy and paste. For complete information, see the *Cisco Content Security Virtual Appliance Installation Guide* available from <http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html>.

This command is available to users with Admin or Operator privileges.

### Usage

Commit: This command does not require a 'commit'.

**Cluster Management:** This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

**Batch Command:** This command does not support a batch format.

## Example

```
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>
```

Errors and hardware misconfigurations may also be shown.

## showlicense

### Description

Displays information about the current virtual email gateway license. Additional details are available using the [featurekey](#) command.

This command is available to users with Admin or Operator privileges.

### Usage

**Commit:** This command does not require a 'commit'.

**Cluster Management:** This command is restricted to machine mode. It is further restricted to the login host (i.e., the specific machine you are logged onto).

**Batch Command:** This command supports a batch format.

### Batch Format

The syntax of this command is: showlicense

## Example

```
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
```

## Geolocation

This section contains the following CLI commands:

### geolocationupdate

#### Description

Manually update the geolocation list.

#### Usage

**Commit:** This command does not require a ‘commit’.

**Cluster Management:** This command is restricted to machine mode.

**Batch Command:** This command supports a batch format. For details, see the inline help by typing the command: `help geolocationupdate`.

#### Example

```
mail3.example.com> geolocationupdate

Requesting update of Geo Countries List.
```

### geolocationstatus

#### Description

Displays the current version of the geolocation list.

#### Usage

**Commit:** This command does not require a ‘commit’.

**Cluster Management:** This command is restricted to machine mode.

**Batch Command:** This command does not support a batch format.

#### Example

```
mail3.example.com> geolocationstatus

Component Version Last Updated
```

Geo Countries List 1.0.48 26 Feb 2017 04:22 (GMT +00:00)

# Configuring Cisco Cloud Service Portal Settings and Usage

This section contains the following CLI command:

- [cloudserviceconfig](#), on page 350

## cloudserviceconfig

- [Description](#), on page 350
- [Usage](#), on page 351
- [Example - Reregistering Email Gateway with Cisco Cloud Services Portal](#), on page 354
- [Example - Enabling Cisco Cloud Services on Email Gateway](#), on page 351
- [Example - Disabling Cisco Cloud Services on Email Gateway](#), on page 351
- [Example - Registering Email Gateway with Cisco Cloud Services Portal](#), on page 352
- [Example - Automatically Registering Email Gateway with Cisco Cloud Services Portal](#), on page 352
- [Example - Deregistering Email Gateway from Cisco Cloud Services Portal](#), on page 353
- [Example - Choosing Cisco Secure Cloud Server to connect Email Gateway to Cisco Cloud Services Portal](#), on page 354
- [Example - Enabling Cisco SecureX Threat Response on Email Gateway](#), on page 355
- [Example - Disabling Cisco SecureX Threat Response on Email Gateway](#), on page 356
- [Example - Enabling CSN on Email Gateway](#), on page 356
- [Example - Disabling CSN on Email Gateway](#), on page 357
- [Example - Downloading Cisco Cloud Services Certificate and Key from Cisco Talos Intelligence Services Portal](#), on page 357

## Description

The `cloudserviceconfig` command is used to:

- Reregister your email gateway with the Cisco Cloud Services portal.
- Enable the Cisco Cloud Services portal on your email gateway.
- Disable the Cisco Cloud Services portal on your email gateway.
- Register your email gateway with the Cisco Cloud Services portal.
- Automatically register your email gateway with the Cisco Cloud Services portal.
- Deregister your email gateway from the Cisco Cloud Services portal.

- Choose the Cisco Secure Cloud server to connect your email gateway to the Cisco Cloud Services portal
- Enable Cisco SecureX or Cisco Threat Response on your email gateway.
- Disable Cisco SecureX or Cisco Threat Response on your email gateway.
- Enable Cisco Success Network (CSN) on your email gateway.
- Disable Cisco Success Network (CSN) on your email gateway.
- Download the Cisco Cloud Services certificate and key from the Cisco Talos Intelligence Services portal.

## Usage

**Commit:** This command does not require a 'commit.'

**Cluster Management:** This command is restricted to the machine mode.

**Batch Command:** This command supports a batch format.

## Example - Enabling Cisco Cloud Services on Email Gateway

In the following example, you can use the `cloudserviceconfig > enable` sub command to enable Cisco Cloud Services on your email gateway.

```
mail1.example.com > cloudserviceconfig

Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable

The Cisco Cloud Service is currently enabled on your appliance.

Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com

Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)

Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1

Selected Cisco Secure Cloud Server is api-sse.cisco.com.

Make sure you run "commit" to make these changes active.
mail1.example.com > commit

Please enter some comments describing your changes:
[]> commit changes

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Dec 29 13:23:19 2020 GMT
mail1.example.com >
```

## Example - Disabling Cisco Cloud Services on Email Gateway

In the following example, you can use the `cloudserviceconfig > disable` sub command to disable Cisco Cloud Services on your email gateway.

**Example - Registering Email Gateway with Cisco Cloud Services Portal**

```

maill.example.com > cloudserviceconfig

The appliance is not registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[> disable

The Cisco Cloud Service is currently disabled on your appliance.
maill.example.com > commit

Please enter some comments describing your changes:
[> commit changes

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Dec 29 13:01:07 2020 GMT
maill.example.com >

```

**Example - Registering Email Gateway with Cisco Cloud Services Portal**

In the following example, you can use the `cloudserviceconfig> register` sub command to register your email gateway with the Cisco Cloud Services portal.




---

**Note** You can only use this sub command if Smart Software licensing is not enabled, and your email gateway is not registered with Cisco Smart Software Manager.

---

```

maill.example.com > cloudserviceconfig

The appliance is not registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[> register

Enter a registration token key to register your appliance with the Cisco Cloud
Service portal.
[> c7fda800adc846792af38d15e4

The appliance registration is in progress.
maill.example.com>

```

**Example - Automatically Registering Email Gateway with Cisco Cloud Services Portal**

In the following example, you can use the `cloudserviceconfig> autoregister` sub command to automatically register your email gateway with the Cisco Cloud Services portal.



**Note** You can only use this sub command, if your email gateway is not automatically registered with the Cisco Cloud Services portal when Smart Software licensing is enabled, and your email gateway is registered with Cisco Smart Software Manager.

```
mail1.example.com> cloudserviceconfig
```

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
  - AUTOREGISTER - register the appliance with the Cisco Cloud Service portal using Smart Licensing Information.
  - ENABLESECUREX - To enable the SecureX feature on your appliance.
  - DISABLECSN - To disable the Cisco Success Network feature on your appliance.
- [> **autoregister**

The auto-registration of the appliance with the Cisco Cloud Service portal is in progress.  
mail1.example.com > cloudserviceconfig

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
  - FETCHCERTIFICATE - Download the Cisco Talos certificate and key
  - ENABLESECUREX - To enable the SecureX feature on your appliance.
  - DISABLECSN - To disable the Cisco Success Network feature on your appliance.
- [>

## Example - Deregistering Email Gateway from Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > deregister` sub command to deregister your email gateway from the Cisco Cloud Services portal.

```
mail1.example.com> cloudserviceconfig
```

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
  - DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
  - SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
  - ENABLESECUREX - To enable the SecureX feature on your appliance.
  - ENABLECSN - To enable the Cisco Success Network feature on your appliance.
- [> **deregister**

Do you want to deregister your appliance from the Cisco Cloud Service portal.

If you deregister, you will not be able to access the Cloud Service features. [N]> yes

**Example - Reregistering Email Gateway with Cisco Cloud Services Portal**

```
The appliance deregistration is in progress.
maill.example.com>
```

**Example - Reregistering Email Gateway with Cisco Cloud Services Portal**

In the following example, you can use the `cloudserviceconfig > reregister` sub command to reregister your email gateway with the Cisco Cloud Services portal.

```
maill.example.com> cloudserviceconfig
```

```
The appliance is successfully registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
```

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

- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
  - DISABLESECUREX - To disable the SecureX feature on your appliance.
  - DISABLECSN - To disable the Cisco Success Network feature on your appliance.
  - REREGISTER - To reregister the appliance with the Cisco Cloud Service portal
- ```
[> reregister
```

```
Currently configured Cisco Cloud Server : api-sse.cisco.com .
Would you like to switch to different server? [Y]> yes
```

```
Available list of Cisco Secure Cloud Servers:
```

1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)

```
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[> 2
```

```
Would you like to proceed with manual registration ? [Y]> yes
```

```
Enter a registration token key to register your appliance with the Cisco Cloud Service
portal.
[> c7fda800afsdffs.....
```

Example - Choosing Cisco Secure Cloud Server to connect Email Gateway to Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > settrs` sub command to choose the required Cisco Secure Cloud Server to connect your email gateway to the Cisco Cloud Services portal.

```
maill.example.com > cloudserviceconfig
```

```
The appliance is not registered with the Cisco Cloud Service portal.
```

```
Currently configured Cisco Cloud Server is api-sse.cisco.com
```

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

- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
 - REGISTER - To register the appliance with the Cisco Cloud Service portal.
 - SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- ```
[> settrs
```

```
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
```

```
Available list of Cisco Secure Cloud Servers:
```

1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)



```
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3

Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.

Make sure you run "commit" to make these changes active.
maill.example.com > commit

Please enter some comments describing your changes:
[]> commit changes

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Dec 29 13:37:40 2020 GMT
maill.example.com >
```

## Example - Enabling Cisco SecureX Threat Response on Email Gateway

In the following example, you can use the `cloudserviceconfig>enablesecurex` sub command to enable Cisco SecureX Threat Response on your email gateway.

```
maill.example.com > cloudserviceconfig

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- ENABLESECUREX - To enable the SecureX feature on your appliance.
- ENABLECSN - To enable the Cisco Success Network feature on your appliance.
[]> enablesecurex

The SecureX feature is currently enabled on your appliance.

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- DISABLESECUREX - To disable the SecureX feature on your appliance.
- ENABLECSN - To enable the Cisco Success Network feature on your appliance.
[]>

maill.example.com > commit

Please enter some comments describing your changes:
[]> commit changes

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Wed Dec 30 00:55:33 2020 GMT
maill.example.com>
```

## Example - Disabling Cisco SecureX Threat Response on Email Gateway

In the following example, you can use the `cloudserviceconfig > disablesecurex` sub command to disable Cisco SecureX Threat Response on your email gateway.

```
maill.example.com > cloudserviceconfig

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- DISABLESECUREX - To disable the SecureX feature on your appliance.
- ENABLECSN - To enable the Cisco Success Network feature on your appliance.
[]> disablesecurex

The SecureX feature is currently disabled on your appliance.

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- ENABLESECUREX - To enable the SecureX feature on your appliance.
- ENABLECSN - To enable the Cisco Success Network feature on your appliance.
[]>

maill.example.com > commit

Please enter some comments describing your changes:
[]> commit changes

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Wed Dec 30 00:58:25 2020 GMT
maill.example.com>
```

## Example - Enabling CSN on Email Gateway

In the following example, you can use the `cloudserviceconfig > enablecsn` sub command to enable CSN on your email gateway.

```
maill.example.com > cloudserviceconfig

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- ENABLESECUREX - To enable the SecureX feature on your appliance.
- ENABLECSN - To enable the Cisco Success Network feature on your appliance.
```

```
[]> enablecsn

The Cisco Success Network feature is currently enabled on your appliance.

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- ENABLESECUREX - To enable the SecureX feature on your appliance.
- DISABLECSN - To disable the Cisco Success Network feature on your appliance.
[]>
```

## Example - Disabling CSN on Email Gateway

In the following example, you can use the `cloudserviceconfig> disablecsn` sub command to disable CSN on your email gateway.

```
mail1.example.com > cloudserviceconfig

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- ENABLESECUREX - To enable the SecureX feature on your appliance.
- DISABLECSN - To disable the Cisco Success Network feature on your appliance.
[]> disablecsn

The Cisco Success Network feature is currently disabled on your appliance.

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
```

## Example - Downloading Cisco Cloud Services Certificate and Key from Cisco Talos Intelligence Services Portal

In the following example, you can use the `cloudserviceconfig> fetchcertificate` sub command to download the Cisco Cloud Services certificate and key from the Cisco Talos Intelligence Services portal.




---

**Note** You can only use this sub command when the existing Cisco Cloud Services certificate is expired and if you have registered your email gateway with Cisco Smart Software Manager.

---

```

mail1.example.com> cloudserviceconfig

The appliance is successfully registered with the Cisco Cloud Service portal.

Currently configured Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key.
- ENABLESECUREX - To enable the SecureX feature on your appliance.
- ENABLECSN - To enable the Cisco Success Network feature on your appliance.
[> fetchcertificate

Current Cisco Talos certificate is valid for 2593 days.

Do you want to overwrite the existing certificate and key [Y][N] ? [> yes

Successfully downloaded the Cisco Talos certificate and key.

mail1.example.com>

```

## Configuring Safe Print Settings on Email Gateway

Use the `scanconfig > safeprint` sub command to configure safe print settings on your email gateway.

### safeprint

- [Description, on page 358](#)
- [Usage, on page 358](#)
- [Example, on page 358](#)

### Description

The `safeprint` sub command is used to configure safe print settings on the email gateway.

### Usage

**Commit:** This command requires a 'commit'.

**Cluster Management:** This command can be used in all three machine modes (cluster, group, machine).

**Batch Command:** This command supports a batch format. For more details, see the inline help by typing the command: `scanconfig safeprint`.

### Example

In the following example, you can use the `safeprint` sub command to configure safe print settings on your email gateway.

```

mail.example.com> scanconfig

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.
- SAFEPRINT - Configure safeprint settings.

[]> safeprint
Enter the maximum attachment size that can safe-print.
[5242880]> 2
Enter the maximum number of pages that you can safe print in an attachment.
[10]> 5
Do you want to use the recommended image quality value to safe print an attachment? [Y]>
yes
Do you want to modify the file types selected to safe print an attachment?
[N]> no
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.
- SAFEPRINT - Configure safeprint settings.

[]>
Mail.example.com> commit
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback?
[Y]> Changes committed: Thu Jul 18 14:24:53 2019 GMT

```

## Connecting the Email Gateway to Talos Cloud Services

This section contains the following CLI commands:

- [talosupdate](#), on page 359
- [talosstatus](#), on page 360

### talosupdate

#### Description

The `talosupdate` command is used to request for an update of the Talos engine.

#### Usage

**Commit:** This command does not require a 'commit'.

**Cluster Management:** This command is restricted to machine mode.

**Batch Command:** This command does not support a batch format.

## Example

```
mail.example.com> talosupdate
Requesting update for Talos components
```

## talosstatus

### Description

The `talosstatus` command displays the version and update status of each updatable component used for communicating to the Talos cloud services.

### Usage

**Commit:** This command does not require a 'commit'.

**Cluster Management:** This command is restricted to machine mode.

**Batch Command:** This command does not support a batch format.

## Example

```
mail.example.com> talosstatus
Component Version Last
Updated
Sender IP Reputation Client 1.0.0-1350252 28 Feb
2020 13:06 (GMT +00:00)
URL Reputation Client 1.0.0-1350252 28 Feb
2020 13:06 (GMT +00:00)
Service Log Client 1.0.0-1350252 28 Feb
2020 13:06 (GMT +00:00)
Talos Engine 1.95.0.220 28 Feb
2020 13:06 (GMT +00:00)
Talos Intelligence Services Module 1.95.0.648 28 Feb
2020 13:06 (GMT +00:00)
Talos-HTTP2 Component 0.9.290 28 Feb
2020 13:06 (GMT +00:00)
Libraries 1.0.0-1350252 28 Feb
2020 13:06 (GMT +00:00)
Protofiles 1.0.0-1350252 28 Feb
2020 13:06 (GMT +00:00)
```

# Integrating the Email Gateway with Cisco Advanced Phishing Protection

- [eaasconfig](#), on page 361
- [eaasupdate](#), on page 361
- [eaasstatus](#), on page 362

## eaasconfig

- [Description, on page 361](#)
- [Usage, on page 361](#)
- [Example - Registering the Email Gateway, on page 361](#)

### Description

Register the email gateway with the Cisco Advanced Phishing Protection cloud service.

### Usage

**Commit:** This command require a 'commit'.

**Cluster Management:** This command can be used in all three machine modes (cluster, group, machine).

**Batch Command:** This command does not support a batch format.

### Example - Registering the Email Gateway

The following example shows a sample configuration to register your email gateway to the Cisco Advanced Phishing Protection cloud service.

```
mail.example.com> eaasconfig

Choose the operation you want to perform:

- REGISTER - To Register the appliance with APP portal

[]> register

Available list of APP region(s) for the registration
1. AMERICA

Select the EAAS region to connect
[]> 1
Enter passphrase obtained from APP portal:
Registration is in progress. Please wait.
Successfully registered the device with APP portal.

Would you like enable APP [Y]> y
```

## eaasupdate

- [Description, on page 361](#)
- [Usage, on page 362](#)
- [Example, on page 362](#)

### Description

Manually request update of the Cisco Advanced Phishing Protection engine.

## Usage

**Commit:** This command does not require a 'commit'.

**Cluster Management:** This command is restricted to machine mode.

**Batch Command:** This command supports a batch format. For more details, see the inline help by typing the command: `eaasupdate force`.

## Example

```
mail.example.com > eaasupdate
Requesting check for new Eaas updates
```

## eaasstatus

- [Description, on page 362](#)
- [Usage, on page 362](#)
- [Example, on page 362](#)

## Description

Manually request update of the Cisco Advanced Phishing Protection engine.

## Usage

**Commit:** This command does not require a 'commit'.

**Cluster Management:** This command is restricted to machine mode.

**Batch Command:** This command does not support a batch format

## Example

```
mail.example.com > eaasstatus

Component Version Last Updated
Advanced Phishing Protection Engine 1.0 Never updated
Advanced Phishing Protection Config 1.0 Never updated
```

# Scanning Password-protected Attachments in Messages

Use the `scanconfig > protectedattachmentconfig` sub command to:

- Enable scanning of password-protected attachments in incoming or outgoing messages.
- Create user-defined passphrases to open password-protected attachments in incoming or outgoing messages.
- Use only user-defined passphrases to open password-protected attachments in incoming or outgoing messages.



- Switch priority of user-defined passphrases.
- Edit user-defined passphrases.
- Delete user-defined passphrases.
- View user-defined passphrases.

## protectedattachmentconfig

- [Description, on page 363](#)
- [Usage, on page 363](#)
- [Example - Enable Scanning of Password-protected Attachments in Incoming and Outgoing Messages, on page 364](#)
- [Example - Creating User-defined Passphrases to Open Password-protected Attachments, on page 365](#)
- [Example - Using Only User-defined Passphrases to Open Password-protected Attachments , on page 366](#)
- [Example - Switching Priority of User-defined Passphrases, on page 368](#)
- [Example - Editing a User-defined Passphrase, on page 369](#)
- [Example - Deleting a User-defined Passphrase, on page 371](#)

## Description

The `protectedattachmentconfig` sub command is used to enable scanning of password-protected attachments in incoming or outgoing messages.

The `protectedattachmentconfig` sub command is used to:

- Enable scanning of password-protected attachments in incoming or outgoing messages.
- Create user-defined passphrases to open password-protected attachments in incoming or outgoing messages.
- Use only user-defined passphrases to open password-protected attachments in incoming or outgoing messages.
- Switch priority of user-defined passphrases.
- Edit user-defined passphrases.
- Delete user-defined passphrases.
- View user-defined passphrases.

## Usage

**Commit:** This sub command requires a 'commit'.

**Cluster Management:** This sub command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command does not support a batch format.

## Example - Enable Scanning of Password-protected Attachments in Incoming and Outgoing Messages

In the following example, you can use the `protectedattachmentconfig` sub command to enable scanning of password-protected attachments in incoming and outgoing messages

```
mail.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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

```
[> protectedattachmentconfig
```

```
Scanning of password-protected attachments for inbound mails: disabled.
Scanning of password-protected attachments for outbound mails: disabled.
```

```
Do you want to scan password-protected attachments for inbound mails?
y/n [N]> yes
```

```
Do you want to scan password-protected attachments for outbound mails?
y/n [N]> yes
```

```
Scanning of password-protected attachments is enabled.
```

```
Do you want to enable user-defined passwords? y/n [N]>
```

```
You will not be able to use user-defined passwords to scan password-protected attachments.
```

```
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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

```
[>
```

```
mail1.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[> changes committed
```

```
Do you want to save the current configuration for rollback? [Y]>
```

```
Changes committed: Wed Nov 04 18:37:42 2020 GMT
```

```
mail1.example.com>
```

## Example - Creating User-defined Passphrases to Open Password-protected Attachments

In the following example, you can use the `protectedattachmentconfig` sub command to create two user-defined passphrases to open password-protected attachments in incoming and outgoing messages.

```
mail.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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

```
[]> protectedattachmentconfig
```

```
Scanning of password-protected attachments for inbound mails: enabled.
Scanning of password-protected attachments for outbound mails: enabled.
```

```
Do you want to scan password-protected attachments for inbound mails? y/n [Y]>
```

```
Do you want to scan password-protected attachments for outbound mails? y/n [Y]>
```

```
Scan password protected attachments configuration unchanged.
```

```
Scanning of password-protected attachments is enabled.
```

```
Do you want to enable user-defined passwords? y/n [Y]> yes
```

```
You can now use user-defined passwords to scan password-protected attachments.
```

```
Choose the operation you want to perform on user-defined passwords.
```

- NEW - Add a new password.

```
[]> new
```

```
Enter a priority for the new password:
```

```
[1]> 1
```

```
Enter the new password:
```

```
[]> example_passphrase@123
```

```
A new password with priority 1 is added.
```

```
Priority: Password:
----- -
1 example_passphrase@123
```

```
Choose the operation you want to perform on user-defined passwords.
```

- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).

```
[]> new
```

## Example - Using Only User-defined Passphrases to Open Password-protected Attachments

```

Priority: Password:
----- -
1 example_passphrase@123

Enter a priority for the new password:
[2]> 2

Enter the new password:
[]> example_passphrase@321

A new password with priority 2 is added.

Priority: Password:
----- -
1 example_passphrase@123
2 example_passphrase@321

Choose the operation you want to perform on user-defined passwords.
- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).
[]>

Do you want to apply user-defined passwords only? y/n [N]>

You can now use both user-defined and extracted passwords from the mail body to
scan password-protected attachments.

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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.
[]>

maill.example.com> commit

Please enter some comments describing your changes:
[]> Changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Mar 11 18:55:16 2021 GMT
maill.example.com>

```

## Example - Using Only User-defined Passphrases to Open Password-protected Attachments

In the following example, you can use the `protectedattachmentconfig` sub command to use only the user-defined passphrases created in [Example - Creating User-defined Passphrases to Open Password-protected Attachments](#) section to open password-protected attachments in incoming and outgoing messages.

```
mail.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.
-SAFEPRINT - Configure safeprint settings.
-PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

[]> protectedattachmentconfig

Scanning of password-protected attachments for inbound mails: enabled.

Scanning of password-protected attachments for outbound mails: enabled.

Do you want to scan password-protected attachments for inbound mails? y/n [Y]>

Do you want to scan password-protected attachments for outbound mails? y/n [Y]>

Scan password protected attachments configuration unchanged.

Scanning of password-protected attachments is enabled.

Do you want to enable user-defined passwords? y/n [Y]>

You can now use user-defined passwords to scan password-protected attachments.

Choose the operation you want to perform on user-defined passwords.
-NEW - Add a new password.
-EDIT - Edit the password.
-SWAP - Swap the priority of the password.
-DELETE - Delete the password.
-PRINT - Print the configured password(s).

Do you want to apply user-defined passwords only? y/n [N]> yes

You can now only use the user-defined passwords to scan password-protected attachments.

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.
-SAFEPRINT - Configure safeprint settings.
-PROTECTEDATTACHMENTCONFIG - Scan password protected attachments. []>

mail.example.com> commit

Please enter some comments describing your changes:
[]> Changes committed

Do you want to save the current configuration for rollback? [Y]>
```

## Example - Switching Priority of User-defined Passphrases

Changes committed: Thu Aug 11 18:55:16 2022 GMT mail1.example.com>

### Example - Switching Priority of User-defined Passphrases

In the following example, you can use the `protectedattachmentconfig` sub command to switch the priority of the first user-defined passphrase with the priority of the second user-defined passphrase.

```
mail.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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

```
[]> protectedattachmentconfig
```

```
Scanning of password-protected attachments for inbound mails: enabled.
Scanning of password-protected attachments for outbound mails: enabled.
```

```
Do you want to scan password-protected attachments for inbound mails? y/n [Y]>
```

```
Do you want to scan password-protected attachments for outbound mails? y/n [Y]>
```

```
Scan password protected attachments configuration unchanged.
```

```
Scanning of password-protected attachments is enabled.
```

```
Do you want to enable user-defined passwords? y/n [Y]> yes
```

```
You can now use user-defined passwords to scan password-protected attachments.
```

```
Choose the operation you want to perform on user-defined passwords.
```

- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).

```
[]> swap
```

```
Priority: Password:
----- -
1 example_passphrase@123
2 example_passphrase@321
```

```
Enter the priority of the first password that you want to switch:
```

```
[]> 1
```

```
Enter the priority of the second password that you want to switch:
```

```
[]> 2
```

```
Passwords with priority 1 and 2 are switched.
```

```

Priority: Password:
----- -
1 example_passphrase@321
2 example_passphrase@123

Choose the operation you want to perform on user-defined passwords.
- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).
[]>

Do you want to apply user-defined passwords only? y/n [N]>

You can now use both user-defined and extracted passwords from the mail body to
scan password-protected attachments.

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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.
[]>

mail.example.com> commit

Please enter some comments describing your changes:
[]> Changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Mar 11 23:07:19 2021 GMT
mail.example.com>

```

## Example - Editing a User-defined Passphrase

In the following example, you can use the `protectedattachmentconfig` sub command to edit a user-defined passphrase.

```

mail.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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

```

## Example - Editing a User-defined Passphrase

```
[]> protectedattachmentconfig

Scanning of password-protected attachments for inbound mails: enabled.
Scanning of password-protected attachments for outbound mails: enabled.

Do you want to scan password-protected attachments for inbound mails? y/n [Y]>
Do you want to scan password-protected attachments for outbound mails? y/n [Y]>

Scan password protected attachments configuration unchanged.

Scanning of password-protected attachments is enabled.

Do you want to enable user-defined passwords? y/n [Y]> yes

You can now use user-defined passwords to scan password-protected attachments.

Choose the operation you want to perform on user-defined passwords.
- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).
[]> edit

Priority: Password:
----- -
1 example_passphrase@321

Enter the password that you want to edit:
[]> example_passphrase@321

Enter the new password:
[example_passphrase@321]> example_passphrase@747

Password with priority 1 is edited.

Priority: Password:
----- -
1 example_passphrase@747

Choose the operation you want to perform on user-defined passwords.
- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).
[]>

Do you want to apply user-defined passwords only? y/n [N]>

You can now use both user-defined and extracted passwords from the mail body to
scan password-protected attachments.

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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.
[]>

mail1.example.com> commit

Please enter some comments describing your changes:
[]> Changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Fri Mar 12 00:05:35 2021 GMT
mail1.example.com>
```

## Example - Deleting a User-defined Passphrase

In the following example, you can use the `protectedattachmentconfig` sub command to delete a user-defined passphrase.

```
mail.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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.

[]> protectedattachmentconfig

Scanning of password-protected attachments for inbound mails: enabled.
Scanning of password-protected attachments for outbound mails: enabled.

Do you want to scan password-protected attachments for inbound mails? y/n [Y]>

Do you want to scan password-protected attachments for outbound mails? y/n [Y]>

Scan password protected attachments configuration unchanged.

Scanning of password-protected attachments is enabled.

Do you want to enable user-defined passwords? y/n [Y]> yes

You can now use user-defined passwords to scan password-protected attachments.

Choose the operation you want to perform on user-defined passwords.
- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
```

```

- DELETE - Delete the password.
- PRINT - Print the configured password(s).
[> delete

Priority: Password:
----- -
1 example_passphrase@321
2 example_passphrase@123

Enter the priority of the password that you want to delete:
[> 2

Password with priority 2 is deleted.

Priority: Password:
----- -
1 Cisco@321

Choose the operation you want to perform on user-defined passwords.
- NEW - Add a new password.
- EDIT - Edit the password.
- SWAP - Swap the priority of the password.
- DELETE - Delete the password.
- PRINT - Print the configured password(s).
[>

Do you want to apply user-defined passwords only? y/n [N]>

You can now use both user-defined and extracted passwords from the mail body to
scan password-protected attachments.

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.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.
[>

maill.example.com> commit

Please enter some comments describing your changes:
[> Changes committed.

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Mar 11 23:51:10 2021 GMT
maill.example.com>

```

## Configuring OpenID Connect 1.0 on Email Gateway for AsyncOS APIs

Use the `oidconfig` command to perform the following tasks:

- Configure OpenID Connect on your email gateway for AsyncOS APIs.
- Delete OpenID Connect configuration settings on your email gateway.

## oidconfig

- [Description, on page 373](#)
- [Usage, on page 373](#)
- [Example - Configuring OpenID Connect for AsyncOS APIs., on page 373](#)
- [Example - Deleting OpenID Connect Configuration Settings on Email Gateway, on page 374](#)

## Description

The `oidconfig` command is used to perform the following tasks:

- Configure OpenID Connect for AsyncOS APIs.
- Delete OpenID Connect configuration settings on your email gateway.

## Usage

**Commit:** This command requires a 'commit.'

**Cluster Management:** This command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command supports a batch format.

## Example - Configuring OpenID Connect for AsyncOS APIs.

In the following example, you can use the `oidconfig` command to configure OpenID Connect on your email gateway for AsyncOS APIs.

```
maill.example.com> oidconfig
```

```
Choose the operation you want to perform:
- SETUP - Configure OpenID Connect for AsyncOS APIs
[]> setup
```

```
Enter the value for metadata URL
The metadata URL is used to fetch the OpenID Connect configuration metadata. The metadata
is used to validate the access token
[]> https://maill.example.com/adfs/.well-known/openid-configuration
```

```
Enter the value for "issuer"
The value must match the issuer claim value of the access token when validating the access
token
[]> http://maill.example.com/adfs/services/trust
```

```
Enter the value for "claim" that contains role information
The value is used to retrieve the role information from the access token.
[]> CiscoMaillAPICaller
```

```
Enter the value for "audience":
Use a comma to separate multiple values
[]> Role
```

**Example - Deleting OpenID Connect Configuration Settings on Email Gateway**

```

Do you want to create an external group mappings? [Y]> yes

Choose the operation you want to perform:
- NEW - Create a new external group mapping.
[]> new

Enter the external group name to map (group names are case-sensitive):
[]> role_map

Assign a role to "role_map":
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]> 1

Mapping for 'role_map' to 'Administrators' created.

Choose the operation you want to perform:
- SETUP - Configure OpenID Connect for AsycOS APIs
- DELETE - Remove OpenID Connect configuration settings
[]>
maill.example.com> commit

Please enter some comments describing your changes:
[]> changes committed

Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Nov 24 06:39:45 2020 GMT
maill.example.com>

```

**Example - Deleting OpenID Connect Configuration Settings on Email Gateway**

In the following example, you can use the `oidconfig` command to delete the OpenID Connect configuration settings on your email gateway.

```

maill.example.com> oidconfig

Choose the operation you want to perform:
- SETUP - Configure OpenID Connect for AsycOS APIs
- DELETE - Remove OpenID Connect configuration settings
[]> delete

Are you sure you want to remove all OpenID Connect
configuration? [N]> yes

Choose the operation you want to perform:
- SETUP - Configure OpenID Connect for AsycOS APIs
[]>

maill.example.com> commit

Please enter some comments describing your changes:
[]> changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Nov 24 06:52:55 2020 GMT
maill.example.com>

```

# Integrating Email Gateway with Cisco Secure Awareness Cloud Service

- [csaconfig](#), on page 375
- [csastatus](#), on page 376
- [csaupdate](#), on page 377

## csaconfig

- [Description](#), on page 375
- [Usage](#), on page 375
- [Example - Enabling Cisco Secure Awareness Cloud Service on Email Gateway](#), on page 375
- [Example - Viewing Details of Repeat Clickers List](#), on page 376
- [Example – Updating the Repeat Clickers List](#), on page 376

## Description

The `csaconfig` command is used to:

- Enable the Cisco Secure Awareness cloud service on your email gateway.
- View details of the Repeat Clickers list.
- Update the Repeat Clickers list.

## Usage

**Commit:** This command requires a 'commit.'

**Cluster Management:** This command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command does not support a batch format.

## Example - Enabling Cisco Secure Awareness Cloud Service on Email Gateway

In the following example, you can use the `csaconfig > enable` sub command to enable the Cisco Secure Awareness cloud service on your email gateway.

```
mail1.example.com> csaconfig
```

```
Choose the operation you want to perform:
- ENABLE - To Enable CSA Service
[]> enable
```

```
Available list of Servers:
1. AMERICAS
2. EUROPE
```

**Example - Viewing Details of Repeat Clickers List**

```

Select the CSA region to connect :
[> 1

Please enter the CSA token for the region selected : de7c55f3ffe94dfb064642

Please specify the Poll Interval
[1d]>

maill.example.com> commit

Please enter some comments describing your changes:
[> changes committed

Do you want to save the current configuration for rollback? [Y]>
Changes committed: Wed Nov 11 18:14:59 2020 GMT

maill.example.com >

```

**Example - Viewing Details of Repeat Clickers List**

In the following example, you can use the `csaconfig> show_list` sub command to view the details of the Repeat Clickers list.

```

maill.example.com > csaconfig

Choose the operation you want to perform:
- EDIT - To edit CSA settings
- DISABLE - To disable CSA service
- UPDATE_LIST - To update the Repeat Clickers list
- SHOW_LIST - To view details of the Repeat Clickers list
[> show_list

List Name : Repeat Clickers
Report ID : 2020
Last Updated : 2020-10-20 11:50:23
List Status : Active

```

**Example – Updating the Repeat Clickers List**

In the following example, you can use the `csaconfig> update_list` sub command to perform an on-demand update or download of the Repeat Clickers list:

```

maill.example.com > csaconfig

Choose the operation you want to perform:
- EDIT - To edit CSA settings
- DISABLE - To disable CSA service
- UPDATE_LIST - To update the Repeat Clickers list
- SHOW_LIST - To view details of the Repeat Clickers list
[> update_list

Machine: maill.example.com An update for the Repeat Clickers list was initiated
successfully

```

**csastatus**

- [Description, on page 377](#)
- [Usage, on page 377](#)
- [Example - Displaying Current Version of Cisco Secure Awareness Components, on page 377](#)

## Description

The `csastatus` command is used to display the current version of the Cisco Secure Awareness components.

## Usage

**Commit:** This command requires a 'commit.'

**Cluster Management:** This command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command does not support a batch format.

## Example - Displaying Current Version of Cisco Secure Awareness Components

In the following example, you can use the `csastatus` command to display the current version of the Cisco Secure Awareness components:

```
mail.example.com> csastatus
Component Version Last Updated
Cisco Secure Awareness Config 1.0.0-0000001 2 Jul 2018 04:22 (GMT +00:00)
Cisco Secure Awareness Engine 1.0.0-0000001 2 Jul 2018 04:22 (GMT +00:00)
```

## csaupdate

- [Description, on page 377](#)
- [Usage, on page 377](#)
- [Example - Manually Updating Cisco Secure Awareness Components, on page 377](#)

## Description

The `csaupdate` command is used to manually update the Cisco Secure Awareness components.

## Usage

**Commit:** This command requires a 'commit.'

**Cluster Management:** This command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command does not support a batch format.

## Example - Manually Updating Cisco Secure Awareness Components

In the following example, you can use the `csaupdate` command to manually update the Cisco Secure Awareness components:

```
mail1.example.com> csaupdate

Requesting check for new CSA updates
mail1.example.com >
```

# Integrating Email Cloud Gateway with Cisco Secure Email Threat Defense

This section contains the following CLI commands:

- [threatdefenseconfig](#), on page 378

## threatdefenseconfig

- [Description](#), on page 378
- [Usage](#), on page 378
- [Example - Enabling Threat Defense Connector](#), on page 378
- [Example - Disabling Threat Defense Connector](#), on page 379

### Description

The `threatdefenseconfig` command is used to configure the settings for Threat Defense Connector.

### Usage

**Commit:** This command requires a 'commit.'

**Cluster Management:** This command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command supports a batch format. See the inline CLI help for more details. Use the help command to access the inline help for this command.

### Example - Enabling Threat Defense Connector

In the following example, you can use the `threatdefenseconfig` command to enable the Threat Defense Connector

```
threatdefenseconfig
```

```
Threat Defense Connector: Disabled
```

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

```
- SETUP - Configure Threat Defense Connector.
```

```
[>] setup
```

```
Threat Defense Connector: Disabled
```

```
Would you like to use Threat Defense Connector? [Y]> Y
```

```
Enter the message intake address retrieved from Cisco Secure Email Threat Defense portal
[test@cisco.com]> testaddress@cisco.com
```

```
Threat Defense Connector: Enabled
```

```
Message Intake Address: testaddress@cisco.com
```



## Example - Disabling Threat Defense Connector

In the following example, you can use the `threatdefenseconfig` command to disable the Threat Defense Connector

```
threatdefenseconfig

Threat Defense Connector: Enabled
Message Intake Address: testaddress@cisco.com

Choose the operation you want to perform:
- SETUP - Configure Threat Defense Connector.
[> setup

Threat Defense Connector: Enabled
Would you like to use Threat Defense Connector? [Y]> n

The system will no longer scan messages for threats using Threat Defense Connector. Are you
sure you want to disable? [N]> y

Threat Defense Connector: Disabled
```

## Creating a File Hash List

Use the `filehashlistconfig` command to:

- Create a file hash list for any one of the following supported file hash types – MD5 or SHA-256.
- Create a file hash list to configure a content filter to take action on messages that contain attachments that match a particular file hash.
- Create a file hash list to use as an exception list for the External Threat Feeds (ETF) feature.

## filehashlistconfig

- [Description, on page 379](#)
- [Usage, on page 380](#)
- [Example - Creating a File Hash List, on page 380](#)

## Description

The `filehashlistconfig` command is used to:

- Create a file hash list for any one of the following supported file hash types – MD5 or SHA-256.
- Create a file hash list to configure a content filter to take action on messages that contain attachments that match a particular file hash.
- Create a file hash list to use as an exception list for the External Threat Feeds (ETF) feature.

## Usage

**Commit:** This sub command requires a 'commit'.

**Cluster Management:** This sub command can be used in all three machine modes (cluster, group, and machine).

**Batch Command:** This command does not support a batch format.

## Example - Creating a File Hash List

In the following example, you can use the `filehashlistconfig` command to create a file hash list.

```
maill.example.com> filehashlistconfig

No file hash lists configured.

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

Enter a name for the file hash list:
> test_file_hash_list

Enter a description for the file hash list:
> Test File Hash List

Enter the type of the file hash list:
1. MD5 checksum(s) only
2. SHA256 checksum(s) only
3. All of the above
Enter the type of the file hash list:
[3]> 2

Enter a list of file hashes separated by commas:
(e.g.: 753710fda3dc815e26cf7d2094d417aab6426b38b99f14e9dd53129e37506e45)
> 753710fda3dc815e26cf7d2094d417aab6426b38b99f14e9dd53129e37506e45

File hash list "myhashlist" added.

Choose the operation you want to perform:
- NEW - Create a new file hash list.
- EDIT - Edit an existing file hash list.
- DELETE - Remove a file hash list.
- PRINT - Display the contents of a file hash list.
[]>
maill.example.com> commit

Please enter some comments describing your changes:
[]> Changes committed

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Fri Mar 12 13:57:52 2021 GMT
maill.example.com>
```



## INDEX

### A

Anti-Spam [319](#)  
HAT parameter [319](#)

### B

bouncing recipients [165](#)  
all [165](#)  
by Envelope From [165](#)  
by hostname [165](#)

### C

case-sensitivity [15](#)  
in CLI [15](#)  
command line interface (CLI) [14–16](#)  
case-sensitivity in [15](#)  
conventions [14](#)  
default setting [14](#)  
exit [16](#)  
history [16](#)  
subcommands [15](#)  
white space [15](#)  
configuration directory [311](#)  
content filters [226](#)  
creating via CLI [226](#)  
CRAM-MD5 [329](#)

### D

delivery queue, monitoring [185](#)  
Domain Keys [70](#)  
DNS TXT record [70](#)

### G

global unsubscribe [187](#)  
adding [187](#)

### H

history, in CLI [16](#)

Host Access Table (HAT) [311](#)  
importing and exporting [311](#)  
order in [311](#)

### L

LDAP [150](#)  
Laser specification [150](#)

### M

maximum [319](#)  
message size in HAT [319](#)  
messages per connection in HAT [319](#)  
recipients per message in HAT [319](#)  
maximum recipients per hour [319](#)

### N

numbers [319](#)

### O

online help [18](#)

### R

refusing connections [311](#)  
rejecting connections [311](#)

### S

SenderBase [319](#)  
SMTP [306, 311](#)  
protocol [306](#)  
relay [311](#)  
SMTP Auth [329](#)  
DIGEST-MD5 [329](#)  
square brackets [14](#)  
SSH [13](#)

T

Telnet [13](#)  
text editor [311](#)