CONTENTS

Preface 1
   Before you Read this Book 1
   Typographic Conventions 2
   Additional Resources 2
      Documentation 2
      Knowledge Base 2
      Cisco Support Community 3
      Customer Support 3
      Registering for a Cisco Account 3
      Cisco Welcomes Your Comments 3

CHAPTER 1
   CLI Quick Reference Guide 1-1
      CLI Commands (No Commit Required) 1-2
      CLI Commands (Commit Required) 1-5

CHAPTER 2
   Command Line Interface: The Basics 2-1
      Accessing the Command Line Interface (CLI) 2-1
      Command Line Interface Conventions 2-2
      General Purpose CLI Commands 2-5
      Batch Commands 2-6
         Batch Command Example 2-6

CHAPTER 3
   The Commands: Reference Examples 3-1
      How to Read the Listing 3-2
      Advanced Malware Protection 3-2
         ampconfig 3-2
      Anti-Spam 3-6
         antispamconfig 3-6
         antispamstatus 3-8
         antispamupdate 3-8
         incomingrelayconfig 3-9
         siblconfig 3-12
 dnshostprefs 3-58  
dnslistconfig 3-59  
dnslisttest 3-60  
dnsstatus 3-60  

General Management/Administration/Troubleshooting 3-61  
  addressconfig 3-62  
  adminaccessconfig 3-64  
  certconfig 3-69  
  date 3-74  
  diagnostic 3-74  
  diskquotaconfig 3-78  
  ecconfig 3-80  
  ecstatus 3-81  
  ecupdate 3-81  
  encryptionconfig 3-81  
  encryptionstatus 3-85  
  encryptionupdate 3-85  
  featurekey 3-86  
  featurekeyconfig 3-87  
  generalconfig 3-87  
  healthcheck 3-88  
  healthconfig 3-89  
  ntpconfig 3-90  
  reboot 3-91  
  repengstatus 3-92  
  resume 3-92  
  resumedeled 3-93  
  resumelistener 3-93  
  revert 3-94  
  settime 3-95  
  settz 3-95  
  shutdown 3-96  
  sshconfig 3-97  
  status 3-99  
  supportrequest 3-100  
  supportrequeststatus 3-102  
  supportrequestupdate 3-103  
  suspend 3-103  
  suspenddel 3-104  
  suspendlistener 3-104
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcpservices</td>
<td>3-105</td>
</tr>
<tr>
<td>techsupport</td>
<td>3-106</td>
</tr>
<tr>
<td>tlsverify</td>
<td>3-107</td>
</tr>
<tr>
<td>trace</td>
<td>3-108</td>
</tr>
<tr>
<td>trackingconfig</td>
<td>3-110</td>
</tr>
<tr>
<td>tzupdate</td>
<td>3-110</td>
</tr>
<tr>
<td>updateconfig</td>
<td>3-111</td>
</tr>
<tr>
<td>updatenow</td>
<td>3-116</td>
</tr>
<tr>
<td>version</td>
<td>3-116</td>
</tr>
<tr>
<td>wipedata</td>
<td>3-117</td>
</tr>
<tr>
<td>upgrade</td>
<td>3-118</td>
</tr>
<tr>
<td>LDAP</td>
<td>3-118</td>
</tr>
<tr>
<td>ldapconfig</td>
<td>3-119</td>
</tr>
<tr>
<td>ldapflush</td>
<td>3-123</td>
</tr>
<tr>
<td>ldaptest</td>
<td>3-124</td>
</tr>
<tr>
<td>sievechar</td>
<td>3-125</td>
</tr>
<tr>
<td>Mail Delivery Configuration/Monitoring</td>
<td>3-126</td>
</tr>
<tr>
<td>addresslistconfig</td>
<td>3-126</td>
</tr>
<tr>
<td>aliasconfig</td>
<td>3-128</td>
</tr>
<tr>
<td>archivemessage</td>
<td>3-130</td>
</tr>
<tr>
<td>altsrchost</td>
<td>3-131</td>
</tr>
<tr>
<td>bounceconfig</td>
<td>3-133</td>
</tr>
<tr>
<td>bouncerecipients</td>
<td>3-136</td>
</tr>
<tr>
<td>bvconfig</td>
<td>3-138</td>
</tr>
<tr>
<td>deleterecipients</td>
<td>3-139</td>
</tr>
<tr>
<td>deliveryconfig</td>
<td>3-140</td>
</tr>
<tr>
<td>delivernow</td>
<td>3-141</td>
</tr>
<tr>
<td>destconfig</td>
<td>3-142</td>
</tr>
<tr>
<td>hostrate</td>
<td>3-149</td>
</tr>
<tr>
<td>hoststatus</td>
<td>3-150</td>
</tr>
<tr>
<td>imageanalysisconfig</td>
<td>3-151</td>
</tr>
<tr>
<td>oldmessage</td>
<td>3-151</td>
</tr>
<tr>
<td>rate</td>
<td>3-153</td>
</tr>
<tr>
<td>redirectrecipients</td>
<td>3-154</td>
</tr>
<tr>
<td>resetcounters</td>
<td>3-155</td>
</tr>
<tr>
<td>removemessage</td>
<td>3-155</td>
</tr>
<tr>
<td>showmessage</td>
<td>3-156</td>
</tr>
<tr>
<td>showrecipients</td>
<td>3-156</td>
</tr>
<tr>
<td>status</td>
<td>3-158</td>
</tr>
<tr>
<td>tophosts</td>
<td>3-159</td>
</tr>
</tbody>
</table>
topin 3-160
unsubscribe 3-160
workqueue 3-162

Networking Configuration / Network Tools 3-162
etherconfig 3-163
interfaceconfig 3-165
nslookup 3-167
netstat 3-168
packetcapture 3-169
ping 3-171
ping6 3-172
routeconfig 3-172
setgateway 3-175
sethostname 3-176
smtproutes 3-176
sslconfig 3-178
sslv3config 3-180
telnet 3-181
traceroute 3-181
traceroute6 3-182

Outbreak Filters 3-184
outbreakconfig 3-184
outbreakflush 3-185
outbreakstatus 3-186
outbreakupdate 3-186

Policy Enforcement 3-187
dictionaryconfig 3-187
exceptionconfig 3-191
filters 3-192
policyconfig 3-194
quarantineconfig 3-217
scanconfig 3-218
stripheaders 3-220
textconfig 3-221

Logging and Alerts 3-224
alertconfig 3-225
displayalerts 3-226
findevent 3-227
grep 3-229
Preface

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

Before you Read this Book

Note
If you have already cabled your appliance to your network, ensure that the default IP address for the appliance 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 appliance.
Typographic Conventions

<table>
<thead>
<tr>
<th>Typeface or Symbol</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>AaBbCc123</td>
<td>The names of commands, files, and directories; on-screen computer output.</td>
<td>Please choose an IP interface for this Listener. The <code>sethostname</code> command sets the name of the appliance.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>What you type, when contrasted with on-screen computer output.</td>
<td><code>mail3.example.com&gt; commit</code> Please enter some comments describing your changes: <code>[]&gt; Changed the system hostname</code></td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Book titles, new words or terms, words to be emphasized. Command line variable; replace with a real name or value.</td>
<td>Read the <em>QuickStart Guide</em>. The appliance <em>must</em> be able to uniquely select an interface to send an outgoing packet. Before you begin, please reset your password to a new value. Old password: <em>ironport</em> New password: <em>your_new_password</em> Retype new password: <em>your_new_password</em></td>
</tr>
</tbody>
</table>

Additional Resources

Documentation

Documentation for your Email Security appliance is available from:


Knowledge Base

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

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

Note

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, page 3.
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 Email Security appliances 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


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:


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.
CLI Quick Reference Guide

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

- CLI Commands (No Commit Required), page 1-2
- CLI Commands (Commit Required), page 1-5
## CLI Commands (No Commit Required)

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
<th>Platform Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>antispamstatus</td>
<td>Display Anti-Spam status</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>antispamupdate</td>
<td>Manually update spam definitions</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>antivirusstatus</td>
<td>Display anti-virus status</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>antivirusupdate</td>
<td>Manually update virus definitions</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>archivemessage</td>
<td>Archives older messages in your queue.</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>bouncerecipients</td>
<td>Bounce messages from the queue</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>clearchanges or clear</td>
<td>Clear changes</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>commit</td>
<td>Commit changes</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>commitdetail</td>
<td>Display detailed information about the last commit</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>date</td>
<td>Display the current date and time</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>deleterecipients</td>
<td>Delete messages from the queue</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>delivernow</td>
<td>Reschedule messages for immediate delivery</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>diagnostic</td>
<td>Check RAID disks, network caches, and SMTP connections. Clear network caches.</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>dig</td>
<td>Look up a record on a DNS server</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>displayalerts</td>
<td>Display the last n alerts sent by the appliance</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>dlprollback</td>
<td>Rollback RSA DLP Engine</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>dlpstatus</td>
<td>Version information for RSA DLP Engine</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>dlpupdate</td>
<td>Update RSA DLP Engine</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>dnsflush</td>
<td>Clear all entries from the DNS cache</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>dnslisttest</td>
<td>Test a DNS lookup for a DNS-based list service</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>dnsstatus</td>
<td>Display DNS statistics</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>ecstatus</td>
<td>Check the version of the enrollment client that is used to obtain certificates</td>
<td>C-Series</td>
</tr>
<tr>
<td>ecupdate</td>
<td>Update the enrollment client that is used to obtain certificates</td>
<td>C-Series</td>
</tr>
<tr>
<td>emdiagnostic</td>
<td>Diagnostic tool for RSA EM on ESA.</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>encryptionstatus</td>
<td>Shows the version of the PXE Engine and Domain Mappings file</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>encryptionupdate</td>
<td>Requests an update to the PXE Engine</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>featurekey</td>
<td>Administer system feature keys</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>findevent</td>
<td>Find events in mail log files</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>graymailstatus</td>
<td>Display the details of existing graymail rules</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>graymailupdate</td>
<td>Manually update graymail rules</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>grep</td>
<td>Search for text in a log file</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>healthcheck</td>
<td>Checks the health of your Email Security appliance</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>help or h or ?</td>
<td>Help</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>hostrate</td>
<td>Monitor activity for a particular host</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Series</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td><code>hoststatus</code></td>
<td>Get the status of the given hostname</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>last</code></td>
<td>Display who has recently logged into the system</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>ldapflush</code></td>
<td>Flush any cached LDAP results</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>ldaptest</code></td>
<td>Perform a single LDAP query test</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>loadlicense</code></td>
<td>Load a virtual appliance license</td>
<td>All virtual appliances</td>
</tr>
<tr>
<td><code>mailconfig</code></td>
<td>Mail the current configuration to an email address</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>nslookup</code></td>
<td>Query a name server</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>netstat</code></td>
<td>Display network connections, routing tables, and network interface statistics.</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>outbreakflush</code></td>
<td>Clear the cached Outbreak Rules</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>outbreakstatus</code></td>
<td>Display current Outbreak Rules</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>outbreakupdate</code></td>
<td>Update Outbreak Filters rules</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>oldmessage</code></td>
<td>Display a list of old messages in the queue</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>packetcapture</code></td>
<td>Intercept and display packets being transmitted or received over the network</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Change your password</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>ping</code></td>
<td>Ping a network host</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>ping6</code></td>
<td>Ping a network host using IPV6</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>quit</code></td>
<td>Quit</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>rate</code></td>
<td>Monitor message throughput</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>reboot</code></td>
<td>Restart the system</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>redirectrecipients</code></td>
<td>Redirect all messages to another relay host</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>removemessage</code></td>
<td>Removes old, undelivered messages from your queue.</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>repengstatus</code></td>
<td>Request version information of Reputation Engine</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>resetconfig</code></td>
<td>Restore the factory configuration defaults</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>resetcounters</code></td>
<td>Reset all of the counters in the system</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>resume</code></td>
<td>Resume receiving and deliveries</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>resumedel</code></td>
<td>Resume deliveries</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>resumelistener</code></td>
<td>Resume receiving</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>revert</code></td>
<td>Revert to a previous release</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>rollovernow</code></td>
<td>Roll over a log file</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>saveconfig</code></td>
<td>Saves the configuration to disk</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Display status of SenderBase queries</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>settime</code></td>
<td>Manually set the system clock</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>showmessage</code></td>
<td>Displays old undelivered messages in your queue.</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td><code>showconfig</code></td>
<td>Display all configuration values</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td><code>showlicense</code></td>
<td>Display virtual appliance license information</td>
<td>All virtual appliances</td>
</tr>
<tr>
<td><code>showrecipients</code></td>
<td>Show messages from the queue by recipient host, Envelope From address, or all messages</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Systems</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shut down the system to power off</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>slbconfig</td>
<td>Configure Safelist/Blocklist settings</td>
<td>C- and X-Series</td>
</tr>
<tr>
<td>status</td>
<td>System status</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>supportrequest</td>
<td>Send a message to Cisco TAC</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>supportrequeststatus</td>
<td>Display Support Request Keywords version information</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>supportrequestupdate</td>
<td>Request manual update for Support Request Keywords</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>suspend</td>
<td>Suspend receiving and deliveries</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>suspenddel</td>
<td>Suspend deliveries</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>suspendlistener</td>
<td>Suspend receiving</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>systemsetup</td>
<td>First time system setup</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>tail</td>
<td>Continuously display the end of a log file</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>techsupport</td>
<td>Allow Cisco TAC to access your system</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>telnet</td>
<td>Connect to a remote host</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>tlsverify</td>
<td>Establish an outbound TLS connection to a remote host and debug any TLS connection issues</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>tophosts</td>
<td>Display the top hosts by queue size</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>topin</td>
<td>Display the top hosts by number of incoming connections</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>trace</td>
<td>Trace the flow of a message through the system</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>traceroute</td>
<td>Display the network route to a remote host</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>traceroute6</td>
<td>Display the network route to a remote host using IPV6.</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>tsupdate</td>
<td>Update timezone rules</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>updatenow</td>
<td>Update all components</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>upgrade</td>
<td>Install an upgrade</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>version</td>
<td>View system version information</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>wipedata</td>
<td>Wipe the core files on the disk and check the status of the last coredump operation</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>webcacheflush</td>
<td>Flush the cache used by the URL filtering feature</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>websecuritydiagnostics</td>
<td>View diagnostic statistics for URL filtering</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>who</td>
<td>List who is logged in</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>whoami</td>
<td>Display your current user id</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>workqueue</td>
<td>Display and/or alter work queue pause status</td>
<td>C- and X- Series</td>
</tr>
</tbody>
</table>
## CLI Commands (Commit Required)

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
<th>Platform Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>addressconfig</td>
<td>Configure From: addresses for system generated mail</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>addresslistconfig</td>
<td>Configure address lists</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>adminaccessconfig</td>
<td>Configure network access list and banner login</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>aggregatorconfig</td>
<td>Configure address of the Cisco Aggregator Server</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>alertconfig</td>
<td>Configure email alerts</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>aliasconfig</td>
<td>Configure email aliases</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>altsrchost</td>
<td>Configure Virtual Gateway™ mappings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>ampconfig</td>
<td>Configure Advanced Malware Protection (File reputation and analysis)</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>antispamconfig</td>
<td>Configure Anti-Spam policy</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>antivirusconfig</td>
<td>Configure anti-virus policy</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>bounceconfig</td>
<td>Configure the behavior of bounces</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>bvconfig</td>
<td>Configure key settings for outgoing mail, and configure how to handle invalid bounces.</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>callaheadconfig</td>
<td>Add, edit, and remove SMTP Call-Ahead profiles</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>certconfig</td>
<td>Configure security certificates and keys</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>clusterconfig</td>
<td>Configure cluster related settings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>deliveryconfig</td>
<td>Configure mail delivery</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>destconfig</td>
<td>Configure options for the Destination Controls Table.</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>dictionaryconfig</td>
<td>Configure content dictionaries</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>diskquotaconfig</td>
<td>Configure disk space</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>dmarcconfig</td>
<td>Configure DMARC settings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>dnsconfig</td>
<td>Configure DNS setup</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>dnshostprefs</td>
<td>Configure IPv4/IPv6 DNS preferences</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>dnslistconfig</td>
<td>Configure DNS List services support</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>domainkeysconfig</td>
<td>Configure DomainKeys support</td>
<td>C-, X- Series</td>
</tr>
<tr>
<td>ecconfig</td>
<td>Configure the enrollment client that is used to obtain certificates</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>emconfig</td>
<td>Configure the RSA Enterprise Manager interoperability settings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>encryptionconfig</td>
<td>Configure email encryption</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>etherconfig</td>
<td>Configure Ethernet settings</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>exceptionconfig</td>
<td>Configure domain exception table</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>featurekeyconfig</td>
<td>Automatically check and update feature keys</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td>filters</td>
<td>Configure message processing options</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>generalconfig</td>
<td>Configure browser settings and other general settings</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>graymailconfig</td>
<td>Configure graymail detection and safe unsubscribe global settings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Series</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>healthconfig</td>
<td>Configure the threshold of various health parameters of your appliance</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>imageanalysisconfig</td>
<td>Configure the IronPort Image Analysis settings</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>incomingrelayconfig</td>
<td>Configure Incoming Relays</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>interfaceconfig</td>
<td>Configure Ethernet IP addresses</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>ldapconfig</td>
<td>Configure LDAP servers</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>listenerconfig</td>
<td>Configure mail listeners</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>loadconfig</td>
<td>Load a configuration file</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>localeconfig</td>
<td>Configure multi-lingual settings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>logconfig</td>
<td>Configure access to log files</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>ntpconfig</td>
<td>Configure NTP time server</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>outbreakconfig</td>
<td>Configure Outbreak Filters</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>policyconfig</td>
<td>Configure per recipient or sender based policies</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>quarantineconfig</td>
<td>Configure system quarantines</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>reportingconfig</td>
<td>Configure reporting settings</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>rollbackconfig</td>
<td>Rollback to one of the previously committed configurations</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>routeconfig</td>
<td>Configure IP routing table</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>scanconfig</td>
<td>Configure attachment scanning policy</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>senderbaseconfig</td>
<td>Configure SenderBase connection settings</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>setgateway</td>
<td>Set the default gateway (router)</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>sethostname</td>
<td>Set the name of the machine</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>settz</td>
<td>Set the local time zone</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>sievechar</td>
<td>Configure characters for Sieve Email Filtering, as described in RFC 3598</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>smimeconfig</td>
<td>Configure S/MIME functionality</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>smtpauthconfig</td>
<td>Configure SMTP Auto profiles</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>smtproutes</td>
<td>Set up permanent domain redirections</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>snmpconfig</td>
<td>Configure SNMP</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>sshconfig</td>
<td>Configure SSH keys</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>sslconfig</td>
<td>Configure SSL settings</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>sslv3config</td>
<td>Enable/Disable SSLv3</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>stripheaders</td>
<td>Set message headers to remove</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>tcpservices</td>
<td>Display information about files opened by processes</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>textconfig</td>
<td>Configure text resources</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>trackingconfig</td>
<td>Configure the tracking system</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>unsubscribe</td>
<td>Update the global unsubscribe list</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>updateconfig</td>
<td>Configure system update parameters</td>
<td>C- and X- Series</td>
</tr>
<tr>
<td>ldap</td>
<td>Configure system upgrade parameters (deprecated command)</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>urllistconfig</td>
<td>Configure whitelists of safe URLs.</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Platform</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>userconfig</td>
<td>Manage user accounts and connections to external authentication sources.</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>websecurityadvancedconfig</td>
<td>Configure advanced settings for URL filtering</td>
<td>C-, X-, and M- Series</td>
</tr>
<tr>
<td>websecurityconfig</td>
<td>Configure global settings for URL filtering</td>
<td>C-, X-, and M- Series</td>
</tr>
</tbody>
</table>
Command Line Interface: The Basics

This chapter contains the following sections:
- Accessing the Command Line Interface (CLI), page 2-1
- Batch Commands, page 2-6

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 appliance. The factory default username and password 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 password for the admin account. The password for the admin account can also be reset directly at any time using the `password` 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 password 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 password below.

Log in to the appliance by entering the username and password below.

**Factory Default Username and Password**

- Username: admin
- Password: ironport

For example:

```
login: admin
password: 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 appliance 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 \texttt{Y}, \texttt{N}, \texttt{Yes}, or \texttt{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 \texttt{NEW}, \texttt{EDIT}, and \texttt{DELETE}. For the \texttt{EDIT} and \texttt{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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Issue the <code>commit</code> command at the command prompt.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Give the <code>commit</code> command the input required.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Receive confirmation of the <code>commit</code> procedure at the CLI.</td>
</tr>
</tbody>
</table>

Changes to configuration that have not been committed will be recorded but not put into effect until the `commit` command is run.
Chapter 2  Command Line Interface: The Basics

Accessing the Command Line Interface (CLI)

Note Not all commands require the commit command to be run. See Chapter 1, “CLI Quick Reference Guide” 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 appliance. 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 appliances 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 Chapter 3, “The Commands: Reference Examples” 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.
Batch Commands

- 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.

[1]> NEW

1. New Sender Group
2. New Policy

[1]> 1

Enter a name for this sender group. (optional)

[1]> REDLIST

Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed.

IP address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are allowed.

Hostnames such as crm.example.com are allowed.

Partial hostnames such as .example.com are allowed.

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

SenderBase Network Owner IDs such as SBO:12345 are allowed.

Remote blacklist queries such as dnslist[query.blacklist.example] are allowed.

Separate multiple hosts with commas

[1]> 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”
The Commands: Reference Examples

This chapter contains the following sections:

- Advanced Malware Protection, page 3-2
- Anti-Spam, page 3-6
- Graymail Detection and Safe Unsubscribing, page 3-13
- Anti-Virus, page 3-15
- Command Line Management, page 3-18
- Configuration File Management, page 3-21
- Cluster Management, page 3-26
- Data Loss Prevention, page 3-28
- S/MIME Security Services, page 3-32
- Domain Keys, page 3-35
- DMARC Verification, page 3-47
- DNS, page 3-52
- General Management/Administration/Troubleshooting, page 3-61
- LDAP, page 3-118
- Mail Delivery Configuration/Monitoring, page 3-126
- Networking Configuration / Network Tools, page 3-162
- Outbreak Filters, page 3-184
- Policy Enforcement, page 3-187
- Logging and Alerts, page 3-224
- Reporting, page 3-241
- Senderbase, page 3-245
- SMTP Services Configuration, page 3-246
- System Setup, page 3-278
- URL Filtering, page 3-283
- User Management, page 3-288
- Virtual Appliance Management, page 3-293
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:

**Step 1** Does the command require a commit command to be implemented on the appliance?

**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 Email Security Appliances*.

For more information about batch formats, please see “Command Line Interface: The Basics” on page 1.

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, page 3-2
- Configure Email Security appliance to Use Public Cloud File Analysis Server, page 3-3
- (Public Cloud File Analysis Services Only) Configuring Appliance Groups, page 3-4
- Configure Email Security appliance to Use an On-Premises File Analysis Server, page 3-5
- Clearing Local File Reputation Cache, page 3-6

**Enabling File Reputation and File Analysis**

```plaintext
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.

[>]

**Configure Email Security appliance 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).
- CLEARCACHE - Clears the local File Reputation cache.
[1]> advanced

Enter cloud query timeout? [15]>

Enter cloud domain? [cloud-domain.com]>

Enter reputation cloud server pool? [cloud-server-pool.com]>

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

Choose a file analysis server:
1. AMERICAS (https://americas-fa.com)
2. Private Cloud [1]>

(Public Cloud File Analysis Services Only) Configuring Appliance Groups

In order to allow all content security 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 appliance 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.
- CLEARCACHE - Clears the local File Reputation cache.
[1]> 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. [1] > 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 Malware Protection

- ADVANCED - Set values for AMP parameters (Advanced configuration).
- VIEWGROUP - view the group members details.
- CLEARCACHE - Clears the local File Reputation cache.

> Note

After you configure an appliance group, you cannot use the setgroup subcommand. If you want to modify the group for any reason, you must open a case with Cisco TAC. You can view the details of the appliance group using the viewgroup subcommand.

Configure Email Security appliance to Use an On-Premises File Analysis Server

```bash
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).
- CLEARCACHE - Clears the local File Reputation cache.

> advanced
Enter cloud query timeout? [15]

Enter cloud domain?
a.immunet.com>

Enter reputation cloud server pool?
cloud-sa.amp.sourcefire.com>

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

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>

Enter heartbeat interval? [15]

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

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.
```
Clearing Local File Reputation Cache

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).
- CLEARCACHE - Clears the local File Reputation cache.

[>] clearcache

Do you want to clear File Reputation Cache? [N]> y

Cache cleared successfully.
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.

[>]

Anti-Spam

This section contains the following commands:

- antispamconfig
- antispamstatus
- antispamupdate
- incomingrelayconfig

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> antispmconfig

Choose the operation you want to perform:
- IRONPORT - Configure IronPort Anti-Spam.
- CLOUDMARK - Configure Cloudmark Service Provider Edition.
- MULTISCAN - Configure IronPort Intelligent Multi-Scan.
[]> ironport

IronPort Anti-Spam scanning: Disabled

Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[]> setup

IronPort Anti-Spam scanning: Disabled

Would you like to use IronPort Anti-Spam scanning? [Y]> y

The IronPort Anti-Spam License Agreement is displayed (if you have not already accepted it).

Do you accept the above IronPort Anti-Spam license agreement? []> Y

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

Never scan message larger than: (Add a trailing K for kilobytes, M for megabytes, or no letters for bytes.)
[1M]>

Always scan message smaller than: (Add a trailing K for kilobytes, M for megabytes, or no letters for bytes.)
[512K]>

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

Would you like to enable regional scanning? [N]> y

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

IronPort Anti-Spam scanning: Enabled

Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[]>
antispamstatus

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.
- CLOUDMARK - Display Cloudmark Service Provider Edition version and rule information.
- MULTISCAN - Display Intelligent Multi-Scan version and rule information.
[]> ironport

<table>
<thead>
<tr>
<th>Component</th>
<th>Last Update</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASE Core Files</td>
<td>Never updated</td>
<td>3.4.0-013</td>
</tr>
<tr>
<td>CASE Utilities</td>
<td>Never updated</td>
<td>3.4.0-013</td>
</tr>
<tr>
<td>Structural Rules</td>
<td>Never updated</td>
<td>3.3.1-009-20141210_214201</td>
</tr>
<tr>
<td>Web Reputation DB</td>
<td>Never updated</td>
<td>20141211_111021</td>
</tr>
<tr>
<td>Web Reputation Rules</td>
<td>Never updated</td>
<td>20141211_111021-20141211_170330</td>
</tr>
<tr>
<td>Content Rules</td>
<td>Never updated</td>
<td>unavailable</td>
</tr>
<tr>
<td>Content Rules Update</td>
<td>Never updated</td>
<td>unavailable</td>
</tr>
</tbody>
</table>

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
- CLOUDMARK - Request updates for Cloudmark Anti-Spam

[]> ironport

Requesting check for new CASE definitions

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

<table>
<thead>
<tr>
<th>relay name</th>
<th>IP address</th>
<th>Header</th>
<th>Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>first-hop</td>
<td>192.168.1.1</td>
<td>Received</td>
<td>[</td>
</tr>
</tbody>
</table>

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.

```
[1]> 192.168.1.2
```

Do you want to use the "Received:" header or a custom header to determine the originating IP address?
1. Use "Received:" header
2. Use a custom header

```
[1]> 2
```

Enter the custom header name that contains the originating IP address:

```
[1]> x-Connecting-IP
```

There are 2 relays defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table

```
[1]> print
```

<table>
<thead>
<tr>
<th>Relay Name</th>
<th>IP Address</th>
<th>Header</th>
<th>Match</th>
<th>Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>First-hop</td>
<td>192.168.1.1</td>
<td>Received</td>
<td>[</td>
<td>1</td>
</tr>
<tr>
<td>Second-hop</td>
<td>192.168.1.2</td>
<td>x-Connecting-IP</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

There are 2 relays defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table

```
[1]> delete
```

1. First-hop: 192.168.1.1
2. Second-hop: 192.168.1.2

Enter the number of the entry you wish to delete:

```
[1]> 1
```

Incoming relay "first-hop" deleted.

There is 1 relay defined.

Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table

```
[1]>
```
slblconfig

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 appliance.
- 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 appliance.

\[ slblconfig export \]

The appliance 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.
[]>

## Graymail Detection and Safe Unsubscribing

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure graymail detection and safe unsubscribing global settings</td>
<td>graymailconfig</td>
</tr>
<tr>
<td>Configuring the incoming mail policy for graymail detection and safe unsubscribing</td>
<td>policyconfig</td>
</tr>
<tr>
<td>Display the details of the existing graymail rules</td>
<td>graymailstatus</td>
</tr>
<tr>
<td>Manually request update of the graymail rules</td>
<td>graymailupdate</td>
</tr>
</tbody>
</table>

### graymailconfig

**Description**

Configure graymail detection and safe unsubscribing global settings.

**Note**

To enable graymail detection and safe unsubscribing, anti-spam scanning must be enabled globally. This can be either the IronPort Anti-Spam or the Intelligent Multi-Scan feature.

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, page 3-215.

**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 graymailconfig`. 

Example

Graymail Detection: Disabled

Choose the operation you want to perform:
- SETUP - Configure Graymail.
{}> setup

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

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

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

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

Graymail Safe Unsubscribe: Disabled

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

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

graymailstatus

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

```bash
mail.example.com> graymailstatus

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graymail Library</td>
<td>01.378.53#15</td>
<td>Never updated</td>
</tr>
<tr>
<td>Graymail Tools</td>
<td>1.0</td>
<td>Never updated</td>
</tr>
</tbody>
</table>
```
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.

Anti-Virus

This section contains the following CLI commands:
- antivirusconfig
- antivirusstatus
- antivirusupdate

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 111.
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 appliance.

```plaintext
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
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.
[>]
```

**Viewing Anti-Virus IDE Details**

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

```plaintext
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
- `Sanyt-A.Ide` Virus Sig. - 22 Dec 2004 06:16:32
- `Bachanan.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

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
IDB 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
- commitdetail
- clearchanges or clear
- help or h or ?
- rollbackconfig
- quit or q or exit

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

<table>
<thead>
<tr>
<th>Previous Commits:</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>committed On</strong></td>
<td><strong>User</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Fri May 23 06:53:43 2014</td>
<td>admin</td>
<td>new user</td>
</tr>
<tr>
<td>Fri May 23 06:50:57 2014</td>
<td>admin</td>
<td>rollback</td>
</tr>
<tr>
<td>Fri May 23 05:47:26 2014</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>
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
- mailconfig
- resetconfig
- saveconfig
- showconfig
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 Email Security Appliances.

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 password option:
1. Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2. Encrypt passwords
3. Plain passwords
[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.
resetconfig

Description

When physically transferring the appliance, 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 appliance is in the offline state. When the resetconfig command completes, the appliance 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.

Warning

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 appliance (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 passwords in the configuration file is encrypted and saved in the `configuration` directory.

```
mail.example.com> saveconfig

Choose the password option:
1. Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2. Encrypt passwords
3. Plain passwords
[1]> 2

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

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 passwords in the configuration are encrypted.

```
mail.example.com> showconfig

Choose the password display option:
1. Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
2. Encrypt passwords
3. Plain passwords
[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.]
```

Cluster Management

This section contains the following CLI commands:

- `clusterconfig`

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.
  
  <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 Email Security Appliances.

Data Loss Prevention

This section contains the following CLI commands:

- dlprollback
- dlpstatus
- dlpupdate
- emconfig
- emdiagnostic

dlprollback

Description

Rollback DLP engine and config to the previous version.

Note

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

Warning

This command will revert your appliance to older DLP policies. You must re-enable DLP policies in Outbound Mail Policies so that DLP scanning can be resumed.
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> dlprollback

This will revert to older DLP policies.
IMPORTANT: After rollback, you must re-enable DLP policies in Outbound Mail Policies so that DLP scanning can be resumed successfully.
Do you wish to rollback? [N]> Y

Requesting rollback for DLP engine.
Re-enable DLP policies in Outbound Mail Policies when rollback is completed (Please check rollback status in mail logs)

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA DLP Engine</td>
<td>3.0.2.31</td>
<td>Never updated</td>
</tr>
</tbody>
</table>

dlpupdate

Description

Update RSA 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.
{}>

emconfig

Description

Configure the interoperability settings for RSA Enterprise Manager.
Note
RSA Enterprise Manager must already be configured via the DLP Global Settings page in the GUI before you can use the `emconfig` command. You cannot enable this functionality using the CLI, only edit the existing settings.

Usage

Commit: This command requires 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.

Batch Format

To set up a connection between the Email Security appliance and RSA Enterprise Manager:

```
emconfig setup [options]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--remote_host</code></td>
<td>Hostname or IP address of the RSA Enterprise Manager.</td>
</tr>
<tr>
<td><code>--remote_port</code></td>
<td>Port to connect to on RSA Enterprise Manager.</td>
</tr>
<tr>
<td><code>--local_port</code></td>
<td>Port on the ESA for Enterprise Manager to connect.</td>
</tr>
<tr>
<td><code>--enable_ssl</code></td>
<td>Enable SSL communication to the RSA Enterprise Manager.</td>
</tr>
<tr>
<td></td>
<td>Use 1 to enable, 0 to disable.</td>
</tr>
</tbody>
</table>

Example of Connecting to RSA Enterprise Manager

```
vm10esa0031.qa> emconfig

RSA Enterprise Manager connection status is: "UNKNOWN"

Choose the operation you want to perform:
- SETUP - Edit RSA Enterprise Manager interop config.
[]> setup

RSA Enterprise Manager: test.example.com:20000
Local port for EM to connect to: 20002
SSL Communication to RSA EM: disabled
Enter hostname of RSA Enterprise Manager: [test.example.com]> em.example.com

Enter port number of RSA Enterprise Manager: [20000]>

Enter local port for EM to connect:
```
Enable SSL communication to EM [N]>

Advanced Settings:
- RSA Enterprise Manager GUID: emlocalsite
- Device Vendor name: Cisco Systems
- Device Status Interval: 5 seconds
- Polling Cycle Interval: 30 seconds
- Connection Throttle Interval: 0 milliseconds
- Max event archive size: 31457280 bytes
- Max files in event archive: 50
- Max file size in event archive: 1048576 MB
- Max size of event.xml file: 1048576 MB
- Interoperability subsystem heartbeat interval: 500 milliseconds
- Heartbeat service attempts before failing: 3
- Connection timeout duration: 30 seconds
- Command status timeout duration: 30 seconds
- Max chunk size: 1000
- Msg exchange cycle: 1

Do you want to change advanced settings? [N]>

Choose the operation you want to perform:
- SETUP - Edit RSA Enterprise Manager interop config.

emdiagnostic

Description

Diagnostic tool for RSA EM on ESA.

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.

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, page 3-33
- Adding a Public Key for Encryption, page 3-34

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.
[1]> 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.
[1]>

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 appliance for encrypting messages.

mail.example.com> smimeconfig

Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.
[1]> gateway

Choose the operation you want to perform:
- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[1]> 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.
[1]> 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-----
MIIdDCCAjIgAwIBAgIBADBQTANBgkqhkiG9w0BAQUFADCBljELMAkGA1UEBhM...
CzAJBgNVBAg...
END CERTIFICATE-----
Domain Keys

This section contains the following CLI commands:

- domainkeysconfig

**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.

**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 3-2  

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Name of domain profile.</td>
</tr>
<tr>
<td>&lt;type&gt;</td>
<td>Type of domain. Can be dk or dkim.</td>
</tr>
<tr>
<td>&lt;domain&gt;</td>
<td>Domain field of domain profile. This forms the d tag of the Domain-Keys signature.</td>
</tr>
<tr>
<td>&lt;selector&gt;</td>
<td>Selector field of domain profile. This forms the s tag of the Domain-Keys signature.</td>
</tr>
<tr>
<td>&lt;user-list&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

[options]

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--key_name</td>
<td>The name of the private key that will be used for signing.</td>
</tr>
<tr>
<td>--canon</td>
<td>The canonicalization algorithm to use when signing by DK. Currently supported algorithms are simple and nofws. Default is nofws.</td>
</tr>
<tr>
<td>--body_canon</td>
<td>The body canonicalization algorithm to use when signing by DKIM. Currently supported algorithms are simple and relaxed. Default is simple.</td>
</tr>
<tr>
<td>--header_canon</td>
<td>The headers canonicalization algorithm to use when signing by DKIM. Currently supported algorithms are simple and relaxed. Default is simple.</td>
</tr>
<tr>
<td>--body_length</td>
<td>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.</td>
</tr>
<tr>
<td>--headers_select</td>
<td>Determines 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. &quot;standard&quot; means to sign predefined set of well known headers such as Subject, From, To, Sender, MIME headers etc. standard_and_custom means to sign well known headers and user-defined set of headers. Default is standard.</td>
</tr>
<tr>
<td>--custom_headers</td>
<td>User-defined set of headers to sign. Is used only in DKIM profiles if headers_select is standard_and_custom. Default is empty set.</td>
</tr>
<tr>
<td>--i_tag</td>
<td>Determines whether to include the i tag into the signature. Possible values are yes or no. Default is yes.</td>
</tr>
</tbody>
</table>
Domain Keys

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>
- headerselect <header_select>
- customheaders <custom_headers>
- itag <i_tag> [<agent_identity>]

---

**Table 3-2** domainkeysconfig New Signing Profile Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--agent_identity</td>
<td>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 &lt;domain&gt;. 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 &lt;domain&gt;.</td>
</tr>
<tr>
<td>--q_tag</td>
<td>Determines whether to include the q tag into the signature. Possible values are yes or no. Default is yes.</td>
</tr>
<tr>
<td>--t_tag</td>
<td>Determines whether to include the t tag into the signature. Possible values are yes or no. Default is yes.</td>
</tr>
<tr>
<td>--x_tag</td>
<td>Determines whether to include the x tag into the signature. Possible values are yes or no. Default is yes.</td>
</tr>
<tr>
<td>--expiration_time</td>
<td>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).</td>
</tr>
<tr>
<td>--z_tag</td>
<td>Determines whether to include the z tag into the signature. Possible values are yes or no. Default is no.</td>
</tr>
</tbody>
</table>
Domain Keys

- 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 appliance:
  
  domainkeysconfig profiles signing export <filename>

- Delete all the signing profiles from the appliance:
  
  domainkeysconfig profiles signing clear

Batch Format - Verification Profiles

- Create a new DKIM verification profile:
  
  domainkeysconfig profiles verification new <name>
  <verification-profile-options>
### Table 3-3  `domainkeysconfig` Verification Profile Options

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--name</td>
<td>The name of DKIM verification profile.</td>
</tr>
<tr>
<td>--min_key_size</td>
<td>The smallest key to be accepted. Possible key-length values (in bits) are 512, 768, 1024, 1536 and 2048. Default is 512.</td>
</tr>
<tr>
<td>--max_key_size</td>
<td>The largest key to be accepted. Possible key-length values (in bits) are 512, 768, 1024, 1536 and 2048. Default is 2048.</td>
</tr>
<tr>
<td>--max_signatures_num</td>
<td>A maximum number of signatures in the message to verify. Possible value is any positive number. Default is 5.</td>
</tr>
<tr>
<td>--key_query_timeout</td>
<td>A number of seconds before the key query is timed out. Possible value is any positive number. Default is 10.</td>
</tr>
<tr>
<td>--max_systemtime_divergence</td>
<td>A number of seconds to tolerate wall clock asynchronization between sender and verifier. Possible value is any positive number. Default is 60.</td>
</tr>
<tr>
<td>--use_body_length</td>
<td>Whether to use a body length parameter. Possible values are yes or no. Default is yes.</td>
</tr>
<tr>
<td>--tempfail_action</td>
<td>The SMTP action should be taken in case of temporary failure. Possible values are accept or reject. Default is accept.</td>
</tr>
<tr>
<td>--tempfail_response_code</td>
<td>The SMTP response code for rejected message in case of temporary failure. Possible value is number in 4xx format. Default is 451.</td>
</tr>
<tr>
<td>--tempfail_response_text</td>
<td>The SMTP response text for rejected message in case of temporary failure. Default is #4.7.5 Unable to verify signature - key server unavailable.</td>
</tr>
<tr>
<td>--permfail_action</td>
<td>The SMTP action should be taken in case of permanent failure. Possible values are accept or reject. Default is accept.</td>
</tr>
<tr>
<td>--permfail_response_code</td>
<td>The SMTP response code for rejected message in case of permanent failure. Possible value is number in 5xx format. Default is 550.</td>
</tr>
<tr>
<td>--permfail_response_text</td>
<td>The SMTP response text for rejected message in case of permanent failure. Default is #5.7.5 DKIM unauthenticated mail is prohibited.</td>
</tr>
</tbody>
</table>

- 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 appliance:
  
  domainkeysconfig profiles verification export <filename>

• Delete all existing verification profiles from the appliance:
  
  domainkeysconfig profiles verification clear

### Batch Format - Signing Keys

• Create a new signing key:
  
  domainkeysconfig keys new <key_name> <key-options>

---

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--generate_key</td>
<td>Generate a private key. Possible key-length values (in bits) are 512, 768, 1024, 1536, and 2048.</td>
</tr>
<tr>
<td>--use_key</td>
<td>Use supplied private key.</td>
</tr>
<tr>
<td>--public_key</td>
<td>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.</td>
</tr>
</tbody>
</table>

• Edit a signing key:
  
  domainkeysconfig keys edit <key_name> key <key-options>
Domain Keys

- 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 appliance:
  
  `domainkeysconfig keys export <filename>`

- Delete all signing keys on the appliance:
  
  `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 appliance:
  
  `domainkeysconfig setup <setup_options>`

  The option available is:
Domain Keys

- `--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 appliance.

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, page 3-45.

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
[ ]>

Enter the size (in bits) of this signing key:
1. 512
2. 768
3. 1024
4. 1536
5. 2048
[ ]>

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

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 DomainKeys signature.

Enter the domain name of the signing domain:

example.com

Selectors are arbitrary names below the ".domainkey." namespace. A selector value and length MUST be legal in the DNS namespace and in email headers with the additional provision that they cannot contain a semicolon. This value becomes the "s" tag of the DomainKeys Signature.

Enter selector:

test

The private key which is to be used to sign messages must be entered. A corresponding public key must be published in the DNS following the form described in the DomainKeys documentation. If a key is not immediately available, a key can be entered at a later time.

Select the key-association method:
1. Create new key
2. Paste in key
3. Enter key at later time
4. Select existing key

[1]> 4

Enter the name or number of a signing key.
1. testkey

[1]>

The canonicalization algorithm is the method by which the headers and content are prepared for presentation to the signing algorithm. Possible choices are "simple" and "relaxed".

Select canonicalization algorithm for body:
1. simple
2. relaxed

[1]> 1

How would you like to sign headers:
1. Sign all existing, non-repeatable headers (except Return-Path header).
2. Sign "well-known" headers (Date, Subject, From, To, Cc, Reply-To, Message-ID, Sender, MIME headers).
3. Sign "well-known" headers plus a custom list of headers.

[2]>

Body length is a number of bytes of the message body to sign. This value becomes the "l" tag of the signature. Which body length option would you like to use?
1. Whole body implied. No further message modification is possible.
2. Whole body auto-determined. Appending content is possible.
3. Specify a body length.

[1]>

Would you like to fine-tune which tags should be used in the DKIM Signature? (yes/no) [N]>

Finish by entering profile users. The following types of entries are allowed:
- Email address entries such as "joe@example.com".
- Domain entries such as "example.com".
- Partial domain entries such as ".example.com". For example, a partial domain of ".example.com" will match "sales.example.com". This sort of entry will not match the root domain ("example.com").
- Leave blank to match all domain users.

Enter user for this signing profile:

[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.
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.

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.

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.

Enter the name or number of a domain profile.
1. Example
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=MIGfMA0GCSqGSGzIBdQEBzUA4GDADCBIQRKPQdX5Dg9J8xBxReA/uPTRY5lCTCqR+qLS5GmlfOplA5u2Bv0
mxZ5Jz+seOT+k7mYD0FSHyNoOv+KCCmY?fRJ3SEO9qLpb1dHev5OCRp/w7hdjPy36PSQJv6v98k5U17
C+DF6XvU1MJSY5sbu2mm9rKAH5m7FWIDQAB;" 

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`

**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]
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Name of the DMARC profile.</td>
</tr>
<tr>
<td>[options]</td>
<td></td>
</tr>
<tr>
<td>--rejectpolicy_action</td>
<td>The message action that AsyncOS must take when the policy in DMARC record is reject. Possible values are “reject”, “quarantine”, or “none.”</td>
</tr>
<tr>
<td>--rejectpolicy_response_code</td>
<td>The SMTP response code for rejected messages. The default value is 550.</td>
</tr>
<tr>
<td>--rejectpolicy_response_text</td>
<td>The SMTP response text for rejected messages. The default value is “#5.7.1 DMARC unauthenticated mail is prohibited.”</td>
</tr>
<tr>
<td>--quarantinepolicy_action</td>
<td>The message action that AsyncOS must take when the policy in DMARC record is quarantine. Possible values are “quarantine” or “none.”</td>
</tr>
<tr>
<td>--quarantinepolicy_quarantine</td>
<td>The quarantine for messages that fail DMARC verification.</td>
</tr>
<tr>
<td>--tempfail_action</td>
<td>The message action that AsyncOS must take on the messages that result in temporary failure during DMARC verification. Possible values are “accept” or “reject.”</td>
</tr>
</tbody>
</table>
DMARC Verification

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--tempfail_response_code</td>
<td>The SMTP response code for rejected messages in case of temporary failure. The default value is 451.</td>
</tr>
<tr>
<td>--tempfail_response_text</td>
<td>The SMTP response text for rejected messages in case of temporary failure. The default value is “#4.7.1 Unable to perform DMARC verification.”</td>
</tr>
<tr>
<td>--permfail_action</td>
<td>The message action that AsyncOS must take on the messages that result in permanent failure during DMARC verification. Possible values are “accept” or “reject.”</td>
</tr>
<tr>
<td>--permfail_response_code</td>
<td>The SMTP response code for rejected messages in case of permanent failure. The default value is 550.</td>
</tr>
<tr>
<td>--permfail_response_text</td>
<td>The SMTP response text for rejected messages in case of permanent failure. The default value is “#5.7.1 DMARC verification failed.”</td>
</tr>
</tbody>
</table>

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]

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--report_schedule</td>
<td>The time when you want AsyncOS to generate DMARC aggregate reports.</td>
</tr>
<tr>
<td>--error_reports</td>
<td>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.</td>
</tr>
<tr>
<td>--org_name</td>
<td>The entity generating DMARC aggregate reports. This must be a domain name.</td>
</tr>
</tbody>
</table>
Chapter 3      The Commands: Reference Examples

DMARC Verification

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 address list: 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.
[>]
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.
DNS

This section contains the following CLI commands:

- `dig`
- `dnsconfig`
- `dnssflush`
- `dnshostprefs`
- `dnslistconfig`
- `dnslisttest`
- `dnssstatus`

**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.
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:

;; 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

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.

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:

  \texttt{dnsconfig parent new} \texttt{<ns_ip>} \texttt{<priority>}

  Command arguments:
  - \texttt{<ns_ip>} - The IP address of the nameserver. Separate multiple IP addresses with commas.
  - \texttt{<priority>} - The priority for this entry.

- Deleting the local nameserver cache:

  \texttt{dnsconfig parent delete} \texttt{<ns_ip>}

- Configuring alternate DNS caches to use for specific domains:

  \texttt{dnsconfig alt new} \texttt{<domains>} \texttt{<ns_ip>}

  Command arguments:
  - \texttt{<ns_ip>} - The IP address of the nameserver. Separate multiple IP addresses with commas.
  - \texttt{<domains>} - A comma separated list of domains.

- Deleting the alternate DNS cache for a specific domain:

  \texttt{dnsconfig alt delete} \texttt{<domain>}

- Configuring DNS to use the Internet root nameservers:

  \texttt{dnsconfig roots new} \texttt{<ns_domain>} \texttt{<ns_name>} \texttt{<ns_ip>}

  Nameserver arguments:
  - \texttt{<ns_domain>} - The domain to override.
  - \texttt{<ns_name>} - The name of the nameserver.
  - \texttt{<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 3-5 Subcommands for dnsconfig Command

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>new</td>
<td>Add a new alternate DNS server to use for specific domains or local DNS server.</td>
</tr>
<tr>
<td>delete</td>
<td>Remove an alternate server or local DNS server.</td>
</tr>
<tr>
<td>edit</td>
<td>Modify an alternate server or local DNS server.</td>
</tr>
<tr>
<td>setup</td>
<td>Switch between Internet root DNS servers or local DNS servers.</td>
</tr>
</tbody>
</table>

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]>

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 appliance 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.
[>

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 appliance 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.

[1]> 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 (192.168.42.24)
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.

dnslisttest

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> dnslisttest
Enter the query server name:
[1]> 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

<table>
<thead>
<tr>
<th>Counters</th>
<th>Reset</th>
<th>Uptime</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Requests</td>
<td>1,115</td>
<td>1,115</td>
<td>1,115</td>
</tr>
<tr>
<td>Network Requests</td>
<td>186</td>
<td>186</td>
<td>186</td>
</tr>
<tr>
<td>Cache Hits</td>
<td>1,300</td>
<td>1,300</td>
<td>1,300</td>
</tr>
<tr>
<td>Cache Misses</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cache Exceptions</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cache Expired</td>
<td>185</td>
<td>185</td>
<td>185</td>
</tr>
</tbody>
</table>

General Management/Administration/Troubleshooting

This section contains the following CLI commands:

- addressconfig
- adminaccessconfig
- certconfig
- date
- diagnostic
- diskquotaconfig
- ecconfig
- ecstatus
- ecupdate
- encryptionconfig
- encryptionstatus
- encryptionupdate
- featurekey
- featurekeyconfig
- generalconfig
- healthcheck
- healthconfig
- ntpconfig
- reboot
- repengstatus
- repengstatus
- resume
- resumedel
- resumelistener
- revert
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

See also Virtual Appliance Management, page 3-293.
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 appliance administrative interface.
- Web interface Cross-Site Request Forgeries protection.
- Option to use host header in HTTP requests.
- Web interface and CLI session inactivity timeout.

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 appliance
  
  `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 appliance
  
  `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 Security appliance. Users can access the appliance 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 appliance after you commit your changes.

In the following example, network access to the appliance 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.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.

`[]> 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 Security appliance to display a message called a “login banner” when a user attempts to log into the appliance 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 appliance. For example, you can create a simple note that saying that unauthorized use of the appliance is prohibited or a detailed warning concerning the organization’s right to review changes made by the user to the appliance.

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 appliance. 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 appliance:

```
mail.example.com> adminaccessconfig
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[>] 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.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.

[>] 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.

mail3.example.com> certconfig

Choose the operation you want to perform:
- CERTIFICATE - 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

[>] certificate

List of Certificates

<table>
<thead>
<tr>
<th>Name</th>
<th>Common Name</th>
<th>Issued By</th>
<th>Status</th>
<th>Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demo</td>
<td>Cisco Appliance Demo</td>
<td>Cisco Appliance Demo</td>
<td>Active</td>
<td>3467 days</td>
</tr>
</tbody>
</table>

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---
MIICLDCCAYCAQAwMQYDVQQIEwdQYXNoZWNrZ3JvdXBsaW5lcy5jKyBzZXJ2ZXIgY2FtcGxl
DQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQKExNleGFtZ3JvdXBsaW5lcyBlZmFjZXIgU2V\n
Paste private key in PEM format (end with '.'): 

---BEGIN RSA PRIVATE KEY---
MIIBPAIBAAJBAL7+aty3S1iBA/+yxjv4q1MUTdi1kNH

Do you want to add an intermediate certificate? [N]> n

List of Certificates
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

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
Enter a name for this certificate profile:
> example.com

Enter Common Name:
> example.com

Enter Organization:
> Example

Enter Organizational Unit:
> Org

Enter Locality or City:
> San Francisco

Enter State or Province:
> CA

Duration before expiration (in days):
> 3650

1. 1024
2. 2048

Enter size of private key:
> 2

Do you want to view the CSR? [Y]>

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCUCAQAwDElkMAgAIUEBhMCVNVxMTA5MDAwMjEwMDAwMDBwNi4xMDkwOTQzLjE=
-----END CERTIFICATE REQUEST-----

List of Certificates
<table>
<thead>
<tr>
<th>Name</th>
<th>Common Name</th>
<th>Issued By</th>
<th>Status</th>
<th>Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.c</td>
<td>example.com</td>
<td>example.com</td>
<td>Valid</td>
<td>3649 days</td>
</tr>
<tr>
<td>partner.c</td>
<td>brutus.partner.com</td>
<td>brutus.partner.com</td>
<td>Valid</td>
<td>30 days</td>
</tr>
<tr>
<td>Demo</td>
<td>Cisco Appliance Demo</td>
<td>Cisco Appliance Demo</td>
<td>Active</td>
<td>3467 days</td>
</tr>
</tbody>
</table>

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
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.

 injured 10esa0031.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 S/MIME certificate and CSR

[1]> 2

Enter a name for this certificate profile:
> s/mime_signing

Enter Common Name:
> CN

Enter Organization:
> ORG

Enter Organizational Unit:
> OU

Enter Locality or City:
> BN

Enter State or Province:
> KA

Enter Country (2 letter code):
> IN

Duration before expiration (in days):

[3650]>

1. 1024
2. 2048

Enter size of private key:

[2]>

Enter email address for 'subjectAltName' extension:
[]> admin@example.com

Add another member? [Y]> n

Begin entering domain entries for 'subjectAltName'.

Enter the DNS you want to add.
[]> domain.com

Add another member? [Y]> n

Do you want to view the CSR? [Y]> n

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
smime_sig  CN                    CN                    Valid          3649 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3329 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[

**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

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

Using the diagnostic Command

The following commands are available within the diagnostic submenu:

<table>
<thead>
<tr>
<th>Option</th>
<th>Sub Commands</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID</td>
<td>1. Run disk verify</td>
<td>Available on C30 and C60 only.</td>
</tr>
<tr>
<td></td>
<td>2. Monitor tasks in progress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Display disk verify verdict</td>
<td></td>
</tr>
<tr>
<td>DISK_USAGE</td>
<td>No Sub Commands</td>
<td>This command has been deprecated. Instead, use the diskquotaconfig command.</td>
</tr>
<tr>
<td>(deprecated)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK</td>
<td>FLUSH</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td></td>
<td>ARPSHOW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SMTPPING</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCPDUMP</td>
<td></td>
</tr>
<tr>
<td>REPORTING</td>
<td>DELETEDDB</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td></td>
<td>DISABLE</td>
<td></td>
</tr>
<tr>
<td>TRACKING</td>
<td>DELETEDDB</td>
<td>C-, X-, and M-Series</td>
</tr>
<tr>
<td></td>
<td>DEBUG</td>
<td></td>
</tr>
<tr>
<td>RELOAD</td>
<td>No Sub Commands</td>
<td>C-, X-, and M-Series</td>
</tr>
</tbody>
</table>

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 arps

• Show the contents of the NDP cache
diagnostic network ndps

• 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.
- SMTPPING - 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.
- SMTPPING - 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.
- SMTPPING – Test a remote SMTP server.
- TCPODUMP – Dump ethernet packets.

[]> smtpping

Enter the hostname or IP address of the SMTP server:
[mall.example.com]> mail.com

The domain you entered has MX records.
Would you like to select an MX host to test instead? [Y]> y

Select an MX host to test.
1. mx00.gmx.com
2. mx01.gmx.com
[1]> 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]> 0

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 Appliance Configuration to the Initial Manufacturer Values

The following example shows how to reset your appliance 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.

[1]> 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

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 Email Security Appliances 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


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

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.
Enteries 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.)
[10M]>

Enter the email address of the encryption account administrator
[administrator@example.com]>

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[>] profiles

Proxy: Not Configured

Profile Name           Key Service          Proxied   Provision Status
--------------------- ---------                -------   ----------------
HIPAA                 Hosted Service        No        Not Provisioned

Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[>] edit

1. HIPAA
Select the profile you wish to edit:
[1]> 1
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date?T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change 'Secure Forward' setting
- REPLYALL - Change 'Secure Reply All' setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages other than English
- 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.

1. High Security (Recipient must enter a password to open the encrypted message, even if credentials are cached ("Remember Me" selected).)
2. Medium Security (No password entry required if recipient credentials are cached ("Remember Me" selected).)
3. No Password Required (The recipient does not need a password to open the encrypted message.)

Please enter the envelope security level:

1

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

Would you like to enable "Secure Forward"? [N]> y

Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: Yes
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages other than English
- 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

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Key Service</th>
<th>Proxied</th>
<th>Provision Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA</td>
<td>Hosted Service</td>
<td>No</td>
<td>Not Provisioned</td>
</tr>
</tbody>
</table>
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 Security appliance, 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

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>PXE Engine</td>
<td>6.7.1</td>
<td>17 Nov 2009 00:09 (GMT)</td>
</tr>
<tr>
<td>Domain Mappings File</td>
<td>1.0.0</td>
<td>Never updated</td>
</tr>
</tbody>
</table>

cipherstatus

Description

The encryptionupdate command requests an update to the PXE Engine on the Email Security appliance.

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.

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 appliances, see also `loadlicense` and `showlicense`.

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
```

<table>
<thead>
<tr>
<th>Module</th>
<th>Quantity</th>
<th>Status</th>
<th>Remaining</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbreak Filters</td>
<td>1</td>
<td>Active</td>
<td>28 days</td>
<td>Tue Feb 25 06:40:53</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IronPort Anti-Spam</td>
<td>1</td>
<td>Dormant</td>
<td>30 days</td>
<td>Wed Feb 26 07:56:57</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sophos Anti-Virus</td>
<td>1</td>
<td>Active</td>
<td>26 days</td>
<td>Sun Feb 23 02:27:48</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bounce Verification</td>
<td>1</td>
<td>Dormant</td>
<td>30 days</td>
<td>Wed Feb 26 07:56:57</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incoming Mail Handling</td>
<td>1</td>
<td>Active</td>
<td>20 days</td>
<td>Sun Feb 16 08:55:55</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IronPort Email Encryption</td>
<td>1</td>
<td>Dormant</td>
<td>30 days</td>
<td>Wed Feb 26 07:56:57</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA Email Data Loss Prevention</td>
<td>1</td>
<td>Active</td>
<td>25 days</td>
<td>Fri Feb 21 10:07:10</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee</td>
<td>1</td>
<td>Dormant</td>
<td>30 days</td>
<td>Wed Feb 26 07:56:57</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:
    - IEOVERRIDE - 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:
    - IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]>

**healthcheck**

**Description**

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

**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 usage

Based on this analysis, we recommend you to contact Cisco Customer Support before upgrading.

healthconfig

Description

Configure the threshold of various health parameters of your appliance 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.

[>] 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.edu

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.

[]> 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)
[]> 1
Currenty configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edu

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.

[]> 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

reboot

Description

Restart the appliance.

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> 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

```bash
mail.example.com> repengstatus
```

<table>
<thead>
<tr>
<th>Component</th>
<th>Last Update</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation Engine</td>
<td>28 Jan 2014 23:47 (GMT +00:00)</td>
<td>1</td>
</tr>
<tr>
<td>Reputation Engine Tools</td>
<td>28 Jan 2014 23:47 (GMT +00:00)</td>
<td>1</td>
</tr>
</tbody>
</table>

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

```bash
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.
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 passwords 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

```

<table>
<thead>
<tr>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 9.1.0-019</td>
</tr>
</tbody>
</table>

Please select an AsyncOS version [1]:
```

Do you want to continue? [N]>
```
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.
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

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> settz
Current time zone: Etc/GMT
Current time zone version: 2010.02.0
Choose the operation you want to perform:
- SETUP - Set the local time zone.

[] > setup

Please choose your continent:
1. Africa
2. America
[ ... ]
11. GMT Offset

[2]> 2

Please choose your country:
1. Anguilla
[ ... ]
45. United States
46. Uruguay
47. Venezuela
48. Virgin Islands (British)
49. Virgin Islands (U.S.)

[45]> 45

Please choose your timezone:
1. Alaska Time (Anchorage)
2. Alaska Time - Alaska panhandle (Juneau)
[ ... ]
21. Pacific Time (Los_Angeles)

[21]> 21

Current time zone: America/Los_Angeles

Choose the operation you want to perform:
- SETUP - Set the local time zone.

[] > shutdown

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

mail3.example.com> shutdown

Enter the number of seconds to wait before abruptly closing connections.
[30]>

System shutting down. Please wait while the queue is being closed.

Closing CLI connection.
Use the power button (in 30 seconds) to turn off the machine.

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.
Reboot. Reboot is required for changes to take effect.

Example

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
>

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

mail.example.com> sshconfig

Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
> sshd

ssh server config settings:
Public Key Authentication Algorithms:
- rsa1
- ssh-dss
- ssh-rsa
Cipher Algorithms:
  aes128-ctr
  aes192-ctr
  aes256-ctr
  arcfour256
  arcfour128
  aes128-cbc
  3des-cbc
  blowfish-cbc
  cast128-cbc
  aes192-cbc
  aes256-cbc
  arcfour
  rijndael-cbc@lysator.liu.se

MAC Methods:
  hmac-md5
  hmac-sha1
  umac-64@openssh.com
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1-96
  hmac-md5-96

Minimum Server Key Size:
  1024

KEX Algorithms:
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group14-sha1
  diffie-hellman-group1-sha1

Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings

[]> setup

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>

Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]>

Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96]>

Enter the Minimum Server Key Size do you want to use
[1024]>

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1]>

ssh server config settings:
Public Key Authentication Algorithms:
  rsa1
  ssh-dss
  ssh-rsa

Cipher Algorithms:
  aes128-ctr
  aes192-ctr
  aes256-ctr
  arcfour256
  arcfour128
  aes128-cbc
3des-cbc
blowfish-cbc
cast128-cbc
aes192-cbc
aes256-cbc
arcfour
rijndael-cbc@lysator.liu.se
MAC Methods:
  hmac-md5
  hmac-sha1
  umac-64@openssh.com
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-shal-96
  hmac-md5-96
Minimum Server Key Size:
  1024
KEX Algorithms:
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group14-sha1
  diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
  []>

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

**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

<table>
<thead>
<tr>
<th>Counters:</th>
<th>Reset</th>
<th>Uptime</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiving</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages Received</td>
<td>62,049,822</td>
<td>290,920</td>
<td>62,049,822</td>
</tr>
<tr>
<td>Recipients Received</td>
<td>62,049,823</td>
<td>290,920</td>
<td>62,049,823</td>
</tr>
<tr>
<td>Rejection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rejected Recipients</td>
<td>3,949,663</td>
<td>11,921</td>
<td>3,949,663</td>
</tr>
<tr>
<td>Dropped Messages</td>
<td>11,606,037</td>
<td>219</td>
<td>11,606,037</td>
</tr>
<tr>
<td>Queue</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Soft Bounced Events</td>
<td>2,334,552</td>
<td>13,598</td>
<td>2,334,552</td>
</tr>
<tr>
<td>Completion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completed Recipients</td>
<td>50,441,741</td>
<td>332,625</td>
<td>50,441,741</td>
</tr>
<tr>
<td>Current IDs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message ID (MID)</td>
<td></td>
<td></td>
<td>99524480</td>
</tr>
<tr>
<td>Injection Conn. ID (ICID)</td>
<td></td>
<td></td>
<td>51180368</td>
</tr>
<tr>
<td>Delivery Conn. ID (DCID)</td>
<td></td>
<td></td>
<td>17550674</td>
</tr>
</tbody>
</table>

Gauges:                  | Current |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections</td>
<td></td>
</tr>
<tr>
<td>Current Inbound Conn.</td>
<td>0</td>
</tr>
<tr>
<td>Current Outbound Conn.</td>
<td>14</td>
</tr>
<tr>
<td>Queue</td>
<td></td>
</tr>
<tr>
<td>Active Recipients</td>
<td>1</td>
</tr>
<tr>
<td>Messages In Work Queue</td>
<td>0</td>
</tr>
<tr>
<td>Kilobytes Used</td>
<td>92</td>
</tr>
<tr>
<td>Kilobytes Free</td>
<td>8,388,516</td>
</tr>
<tr>
<td>Quarantine</td>
<td></td>
</tr>
<tr>
<td>Messages In Quarantine</td>
<td>0</td>
</tr>
<tr>
<td>Policy, Virus and Outbreak</td>
<td></td>
</tr>
<tr>
<td>Kilobytes In Quarantine</td>
<td>0</td>
</tr>
<tr>
<td>Policy, Virus and Outbreak</td>
<td></td>
</tr>
</tbody>
</table>

**supportrequest**

**Description**

Send a message to Cisco customer support. This command requires that the appliance 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 appliance, your Cisco.com user ID must be associated with your service agreement contract for this appliance. 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/autho/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 (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

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 [3]
4. Email Security Appliance - Virtual [1]>

Please select the problem category:
1. Upgrade
2. Operate
3. Configure
4. Install [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

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:  
How to associate your CCO ID with contract:  
https://tools.cisco.com/RPFA/profile/profile_management.do
Frequently Asked Question:  

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 '0', '.', '-', 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.
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

Example

```
30>
30> Enter the number of seconds to wait before abruptly closing connections.
30> Waiting for listeners to exit...
30> Receiving suspended.
30> 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)
ftpdm.main    - The FTP daemon
rnetd         - The INET daemon
interface     - The interface controller for inter-process communication
ipfw          - The IP firewall
slapd         - The Standalone LDAP daemon
snmp          - The SNMP 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

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>USER</th>
<th>TYPE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>root</td>
<td>IPv4</td>
<td>127.0.0.1:53</td>
<td></td>
</tr>
<tr>
<td>postgres</td>
<td>postgres</td>
<td>IPv4</td>
<td>127.0.0.1:5432</td>
<td></td>
</tr>
<tr>
<td>qabackdo</td>
<td>root</td>
<td>IPv4</td>
<td>*:8123</td>
<td></td>
</tr>
<tr>
<td>ftpdm.main</td>
<td>root</td>
<td>IPv4</td>
<td>10.1.1.0:21</td>
<td></td>
</tr>
<tr>
<td>euq_webui</td>
<td>root</td>
<td>IPv4</td>
<td>10.1.1.0:83</td>
<td></td>
</tr>
<tr>
<td>euq_webui</td>
<td>root</td>
<td>IPv6</td>
<td>[2001:db8::]:83</td>
<td></td>
</tr>
<tr>
<td>gui</td>
<td>root</td>
<td>IPv4</td>
<td>172.29.181.70:80</td>
<td></td>
</tr>
<tr>
<td>gui</td>
<td>root</td>
<td>IPv4</td>
<td>10.1.1.0:80</td>
<td></td>
</tr>
<tr>
<td>gui</td>
<td>root</td>
<td>IPv6</td>
<td>[2001:db8::]:80</td>
<td></td>
</tr>
<tr>
<td>gui</td>
<td>root</td>
<td>IPv4</td>
<td>172.29.181.70:443</td>
<td></td>
</tr>
<tr>
<td>gui</td>
<td>root</td>
<td>IPv4</td>
<td>10.1.1.0:443</td>
<td></td>
</tr>
</tbody>
</table>
```
### 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: XXXXXXXXXX-XXXXXXX

Choose the operation you want to perform:
- DISABLE - Prevent customer service representatives from remotely accessing your system.
- STATUS - Display the current techsupport status.

\[
\text{tlsverify}
\]

**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 mxe.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.dom
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:sNH70"
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).
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 Appliance to Download Updates from Updater Servers, page 3-111
- Configure the Appliance to Verify the Validity of Updater Server Certificate, page 3-114
- Configure the Appliance to Trust Proxy Server Communication, page 3-115

Configure the Appliance to Download Updates from Updater Servers

In the following example, the updateconfig command is used to configure the appliance 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):

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):

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

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

[1]> setup

For the following services, please select where the system will download updates from:
Service (images):

------------------------------------------------------------------------------------------
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):

------------------------------------------------------------------------------------------
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):

------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades  Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own server

[1]>

For the following services, please select where the system will download the list of available updates from:

Service (list):                                  Update URL:

------------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                          Cisco IronPort Servers
Support Request updates                           Cisco IronPort Servers

1. Use Cisco IronPort update servers
2. Use own update list

[1]>

For the following services, please select where the system will download the list of available updates from:

Service (list):                                  Update URL:

------------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                  Cisco IronPort Servers

1. Use Cisco IronPort update servers
2. Use own update list

[1]>

Enter the time interval between checks for new:
- Timezone rules
  - Enrollment Client Updates (used to fetch certificates for URL Filtering)
  - Support Request updates
Use a trailing 's' for seconds, 'm' for minutes or 'h' for hours. The minimum valid update time is 30s or enter '0' to disable automatic updates (manual updates will still be available for individual services).

[5m]>

When initiating a connection to the update server the originating IP interface is chosen automatically. If you want to choose a specific interface, please specify it now.
1. Auto
2. Management (10.76.69.149/24: vm30esa0086.ibqa)

[1]>

Do you want to set up a proxy server for HTTP updates for ALL of the following services:
- Feature Key updates
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
- Cisco IronPort AsyncOS upgrades

[N]>

Do you want to set up an HTTPS proxy server for HTTPS updates for ALL of the following services:
- Feature Key updates
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
- Cisco IronPort AsyncOS upgrades
- SenderBase Network Participation sharing
Configure the Appliance to Verify the Validity of Updater Server Certificate

If you configure this option, every time the appliance 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
```

If you configure this option, every time the appliance communicates with 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 Update Logs. The following example shows how to configure this option:

```
mail.example.com> updateconfig
```

Configure the Appliance to Verify the Validity of Updater Server Certificate

If you configure this option, every time the appliance 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 Update Logs. The following example shows how to configure this option:

```
mail.example.com> updateconfig
```

Configure the Appliance to Verify the Validity of Updater Server Certificate

If you configure this option, every time the appliance 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 Update Logs. The following example shows how to configure this option:

```
mail.example.com> updateconfig
```

Configure the Appliance to Verify the Validity of Updater Server Certificate

If you configure this option, every time the appliance 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 Update Logs. The following example shows how to configure this option:

```
mail.example.com> updateconfig
```

Configure the Appliance to Verify the Validity of Updater Server Certificate

If you configure this option, every time the appliance 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 Update Logs. The following example shows how to configure this option:

```
mail.example.com> updateconfig
```
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

Should server certificates from Cisco update servers be validated? [Yes]>

Service (images):
------------------------------------------------------------------------------------------
Feature Key updates                                    Update URL: 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):
------------------------------------------------------------------------------------------
Timezone rules                                         Cisco IronPort Servers
Enrollment Client Updates                               Cisco IronPort Servers
Support Request updates                                 Cisco IronPort Servers

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

Choose the operation you want to perform:

Configure the Appliance 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 appliance. By doing so, the appliance trusts the proxy server communication. The following example shows how to configure this option:

...
- 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-----
MIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMKSzCC
END CERTIFICATE-----
.

Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[>] 

updatenow

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 appliance 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

Upgrades available:
1. AsyncOS (**DON'T TOUCH!***) 4.0.8 upgrade, 2005-05-09 Build 900
2. AsyncOS 4.0.8 upgrade, 2005-08-12 Build 030
........
45. SenderBase Network Participation Patch

[45]> Performing an upgrade will require a reboot of the system after the upgrade is applied. Do you wish to proceed with the upgrade? [Y]> Y

LDAP

This section contains the following CLI commands:
- ldapconfig
- ldapflush
- ldaptest
- sievechar
ldapconfig

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 ldapconfig command is used to define an LDAP server for the appliance 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. Password based
[]> 2

Please enter the bind username: [cn=Anonymous]>
Please enter the bind password:
[]>

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: password
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: password
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.
- CERTAUTH - Configure certificate authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
Example: LDAP

[>] ldaprouting

Please create a name for this query:

[PublicLDAP.routing]> PublicLDAP.routing

Enter the LDAP query string:

[(mailLocalAddress=\{a\})] > (mailLocalAddress=(a))

The query requires one of the attributes below. Please make a selection.

[1] Configure MAILROUTINGADDRESS only - Rewire the Envelope Recipient (and leave MAILHOST unconfigured)?

[2] Configure MAILHOST only - Send the messages to an alternate mail host (and leave MAILROUTINGADDRESS unconfigured)?

[3] Configure both attributes

[>] 1

Enter the attribute which contains the full rfc822 email address for the recipients.

[mailRoutingAddress]> mailRoutingAddress

Do you want to test this query? [Y]> n

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing

Choose the operation you want to perform:

- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.

[>] masquerade

Please create a name for this query:

[PublicLDAP.masquerade]> PublicLDAP.masquerade

Enter the LDAP query string:

[(mailRoutingAddress=\{a\})] > (mailRoutingAddress=(a))

Enter the attribute which contains the externally visible full rfc822 email address.

[>] mailLocalAddress

Do you want the results of the returned attribute to replace the entire friendly portion of the original recipient? [N]> n

Do you want to test this query? [Y]> n

Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: password
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})]

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

Password to use in query:
[>] password

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: password
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

LDAP will determine the interface automatically.

Should group queries that fail to complete be silently treated as having negative results? [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

No LDAP server configurations.

Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.

ldapflush

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.ldapaccept
[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.ldapaccept
[1]> 1
```
Address to use in query:
[]> bogus@example.com

LDAP query test results:
Query: PublicLDAP.ldapaccept
Argument: bogus@example.com
Action: drop or bounce (depending on listener settings)
Reason: no matching LDAP record was found
LDAP query test finished.
mail3.example.com>

**sievechar**

**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
- aliasconfig
- archivemessage
- altsrhost
- bounceconfig
- bouncerecipients
- bvconfig
- deleterecipients
- deliveryconfig
- delivernow
- destconfig
- hostrate
- hoststatus
- imageanalysisconfig
- oldmessage
- rate
- redirectrecipients
- resetcounters
- removemessage
- showmessage
- showrecipients
- status
- tophosts
- topin
- unsubscribe
- workqueue

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**

```plaintext
mail.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.

Do you want to enter only full Email Addresses? [N]> Y

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-existant 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 appliance:

```
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.
```
räu  print

admin: administrator@example.com

[ example.com ]
customeercare: 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>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain&gt;</td>
<td>The domain context in which an alias is applied. ‘Global’ specifies the Global Domain Context.</td>
</tr>
<tr>
<td></td>
<td>The name of the alias to configure</td>
</tr>
<tr>
<td></td>
<td>Aliases permitted at the Global Domain Context:</td>
</tr>
<tr>
<td></td>
<td>‘user@domain’ — This email address.</td>
</tr>
<tr>
<td></td>
<td>‘user’— This user for any domain.</td>
</tr>
<tr>
<td></td>
<td>‘@domain— All users in this domain.</td>
</tr>
<tr>
<td></td>
<td>‘@.partialdomain’— All users in this domain or any of its sub-domains.</td>
</tr>
<tr>
<td></td>
<td>Aliases permitted for specific domain contexts:</td>
</tr>
<tr>
<td></td>
<td>‘user’— This user in this domain context</td>
</tr>
<tr>
<td></td>
<td>‘user@domain’— This email address</td>
</tr>
<tr>
<td>&lt;email_address&gt;</td>
<td>The email address that an alias maps to. A single alias can map to multiple email addresses.</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>The filename to use with importing/exporting the alias table.</td>
</tr>
</tbody>
</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
```

altsrchost

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 altsrchost 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 altsrchost mappings are printed to confirm and the changes are committed.

```
mail3.example.com> altsrchost
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 "user0" 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)

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.

[1]> 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.

[1]> 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.

[1]> 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.

[1]> mail3.example.com > commit

Please enter some comments describing your changes:

[1]> Added 2 altsrchost 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 does not support a batch format.

**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

If a message is undeliverable after some interval, do you want to send a delay warning message? (Yes/No/Default) [N]> y

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.

\[1]> bounce-mailbox@example.com

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.

\[1]> mail3.example.com>

---

**Editing the Default Bounce Profile**

You can also edit the default bounce profile. In this example, the default profile is edited to increase the maximum number of seconds to wait before retrying unreachable hosts from 3600 (one hour) to 10800 (three hours):

mail3.example.com> bounceconfig

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.

\[1]> edit

Please enter the number of the profile to edit:

\[1]> 2

Please enter the maximum number of retries.

\[100]> 

Please enter the maximum number of seconds a message may stay in the queue before being hard bounced.

\[259200]> 

Please enter the initial number of seconds to wait before retrying a message.

\[60]> 

Please enter the maximum number of seconds to wait before retrying a message.

\[3600]> 10800

Do you want a message sent for each hard bounce? (Yes/No/Default) \[Y]> 

Do you want bounce messages to use the DSN message format? (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]>

---

CLI Reference Guide for AsyncOS 9.6 for Cisco Email Security Appliances
Do you want hard bounce messages sent to an alternate address, instead of the sender? [Y]>

Please enter the email address to send hard bounce.

[bounce-mailbox@example.com]>

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.

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.

[]> 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 exampe 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 appliance 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
```

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

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

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 MX or 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>
<thead>
<tr>
<th>Domain</th>
<th>Conn. Limit</th>
<th>Rcpt. Limit</th>
<th>Min. Prd.</th>
<th>Enforce MX/DOM</th>
</tr>
</thead>
<tbody>
<tr>
<td>(default)</td>
<td>500</td>
<td>None</td>
<td>1</td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Unlisted domains get their own set of 500 connections with unlimited rcpts/hr</td>
</tr>
<tr>
<td>(default)</td>
<td>500</td>
<td>None</td>
<td>1</td>
<td>MXIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mail gateways at unlisted domains get up to 500 connections, with unlimited rcpts/hr</td>
</tr>
<tr>
<td>partner.com</td>
<td>10</td>
<td>500</td>
<td>60</td>
<td>Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>All gateways at partner.com will share 10 connections, with 500 rcpts/minute maximum</td>
</tr>
<tr>
<td>101.202.101.2</td>
<td>500</td>
<td>None</td>
<td>0</td>
<td>MXIP</td>
</tr>
</tbody>
</table>

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.

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Rate Limiting</th>
<th>TLS</th>
<th>Bounce Verification</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
<td>(Default)</td>
</tr>
</tbody>
</table>

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]> 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 “Editing the Default Bounce Profile” on page 134) 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 apply a specific bounce verification address tagging setting for this domain? [N]> y

Perform bounce verification address tagging? [N]> y
Do you wish to apply a specific bounce profile to this domain? [N]> y
Please choose a bounce profile to apply:
1. Default
2. New Profile

[1]> 1

There are currently 2 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- 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]> detail

<table>
<thead>
<tr>
<th>Domain</th>
<th>Rate Limiting</th>
<th>TLS</th>
<th>Bounce Verification</th>
<th>Bounce Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>newpartner.com</td>
<td>Default</td>
<td>Req</td>
<td>On</td>
<td>Default</td>
</tr>
<tr>
<td>(Default)</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
<td>(Default)</td>
</tr>
</tbody>
</table>

Enter the domain name to view, or enter DEFAULT to view details for the default, or enter ALL to view details for all:

[1]> 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.

[1]> mail3.example.com> commit

Please enter some comments describing your changes:

[1]> 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 appliance 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`.
```
[1]> 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.
**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.
[1]> setup
```

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
```

Do you want to send an alert when a required TLS connection fails? [N]> 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:
[1]> aol.com

Enter the number of seconds between displays.
[10]> 1

<table>
<thead>
<tr>
<th>Time</th>
<th>Host Status</th>
<th>CrtCncOut</th>
<th>ActvRcpi</th>
<th>ActvRcp</th>
<th>DlvRcpi</th>
<th>HrdBncRcpi</th>
<th>SftBncEvt</th>
</tr>
</thead>
<tbody>
<tr>
<td>23:38:23</td>
<td>up</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23:38:24</td>
<td>up</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23:38:25</td>
<td>up</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

^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’.
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:
[1]> 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 ActivityWed Nov 13 13:47:02 2003
  Recipients0
=================================================================================
example.com (PublicNet_023):
  Host up/down:up
  Last ActivityWed 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.
```

<table>
<thead>
<tr>
<th>Time</th>
<th>Connections</th>
<th>Recipients</th>
<th>Recipients</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In</td>
<td>Out</td>
<td>Received</td>
<td>Delta</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
redirectrecipients

Description

Redirect all messages to another relay host.

⚠️ Warning

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.

⚠️ 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.

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
mail3.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
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>
  ```

  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/Recipient/Subject
[RID][Atmps]Recipient
15271230user123456@ironport.comTesting
[0][0]9554@example.com
15221230user123456@ironport.comTesting
[0][0]3059@example.com
15291230user123456@ironport.comTesting
[0][0]7284@example.com
15301230user123456@ironport.comTesting
[0][0]8243@example.com
15321230user123456@ironport.comTesting
[0][0]1820@example.com
15311230user123456@ironport.comTesting
[0][0]9595@example.com
15181230user123456@ironport.comTesting
[0][0]8778@example.com
15351230user123456@ironport.comTesting
```

status

The status command is used to display the system status of your appliance. Using the ‘detail’ option (status detail) displays additional 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> status detail

Status as of:                Mon Sep  8 00:01:44 2014 GMT
Up since:                    Tue Aug 26 17:24:16 2014 GMT

(12d 6h 37m 28s)
Last counter reset:          Never
System status:               Online
Oldest Message:              No Messages
Feature - IronPort Anti-Spam: 1459 days
Feature - Incoming Mail Handling: Perpetual
Feature - Outbreak Filters:  1459 days

Counters:                               Reset          Uptime        Lifetime
Receiving
   Messages Received                       2               2               2
   Recipients Received                     2               2               2
Rejection
   Rejected Recipients                     0               0               0
   Dropped Messages                        0               0               0
Queue
   Soft Bounced Events                     0               0               0
Completion
   Completed Recipients                    0               0               0
Current IDs
   Message ID (MID)                        2
   Injection Conn. ID (ICID)               0
   Delivery Conn. ID (DCID)                13

Gauges:                                      Current
Connections
   Current Inbound Conn.                   0
   Current Outbound Conn.                  0
Queue
   Active Recipients                       2
   Messages In Work Queue                  0
Kilobytes Used                                      184  
Kilobytes Free                                      8,388,424  
Quarantine  
Messages In Quarantine  
  Policy, Virus and Outbreak                      0  
Kilobytes In Quarantine  
  Policy, Virus and Outbreak                      0  

tophosts

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.

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> 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.

1*  example.com         2             0      0       0             0             0
2   the.encryption.queue 0             0      0       0             0             0
3   the.euq.queue       0             0      0       0             0             0
4   the.euq.release.queue 0             0      0       0             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**

```bash
mail3.example.com> topin
Status as of: Sat Aug 23 21:50:54 2003

<table>
<thead>
<tr>
<th>#</th>
<th>Remote hostname</th>
<th>Remote IP addr.</th>
<th>listener</th>
<th>Conn. In</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mail.remotedomain01.com</td>
<td>172.16.0.2</td>
<td>Incoming01</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>mail.remotedomain02.com</td>
<td>172.16.0.2</td>
<td>Incoming02</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>mail.remotedomain03.com</td>
<td>172.16.0.4</td>
<td>Incoming01</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>mail.remotedomain04.com</td>
<td>172.16.0.5</td>
<td>Incoming02</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>mail.remotedomain05.com</td>
<td>172.16.0.6</td>
<td>Incoming01</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>mail.remotedomain06.com</td>
<td>172.16.0.7</td>
<td>Incoming02</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>mail.remotedomain07.com</td>
<td>172.16.0.8</td>
<td>Incoming01</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>mail.remotedomain08.com</td>
<td>172.16.0.9</td>
<td>Incoming01</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>mail.remotedomain09.com</td>
<td>172.16.0.10</td>
<td>Incoming01</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>mail.remotedomain10.com</td>
<td>172.16.0.11</td>
<td>Incoming01</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>mail.remotedomain11.com</td>
<td>172.16.0.12</td>
<td>Incoming01</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>mail.remotedomain12.com</td>
<td>172.16.0.13</td>
<td>Incoming02</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>mail.remotedomain13.com</td>
<td>172.16.0.14</td>
<td>Incoming01</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>mail.remotedomain14.com</td>
<td>172.16.0.15</td>
<td>Incoming01</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>mail.remotedomain15.com</td>
<td>172.16.0.16</td>
<td>Incoming01</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>mail.remotedomain16.com</td>
<td>172.16.0.17</td>
<td>Incoming01</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>mail.remotedomain17.com</td>
<td>172.16.0.18</td>
<td>Incoming01</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>mail.remotedomain18.com</td>
<td>172.16.0.19</td>
<td>Incoming02</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>mail.remotedomain19.com</td>
<td>172.16.0.20</td>
<td>Incoming01</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>mail.remotedomain20.com</td>
<td>172.16.0.21</td>
<td>Incoming01</td>
<td>1</td>
</tr>
</tbody>
</table>
```

### 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 appliance 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
[]> 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
```
Networking Configuration / Network Tools

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
- interfaceconfig
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.
- LOOBACK - View and configure Loopback.
- MTU - View and configure MTU.
[]> vlan

VLAN interfaces:

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

VLAN tag ID for the interface (Ex: '34'):
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.
[1]>

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.
[1]>

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.
[1]> loopback

Currently configured loopback interface:

Choose the operation you want to perform:
- ENABLE - Enable Loopback Interface.
[1]>

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.
[1]> 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.
[1]> edit

Enter the name or number of the ethernet interface you wish to edit. 
[1]> pair1

That value is not valid.

Enter the name or number of the ethernet interface you wish to edit. 
[1]> 12

That value is not valid.

Enter the name or number of the ethernet interface you wish to edit. 
[1]> 2

Please enter a non-default (1500) MTU value for the Data 2 interface. 
[1]> 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>
--ip=IPv4 Address/Netmask
--ip6=IPv6 Address/Prefix Lenght
[--ftp=<port>]
[--telnet=<port>]
[--ssh=<port>]
[--http=<port>]
[--https=<port>]
[--euq_http=<port>]


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]

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

Hostname: [mail.example.com]

Do you want to enable SSH on this interface? [Y]

Which port do you want to use for SSH? [22]

Do you want to enable FTP on this interface? [N]

Do you want to enable Cluster Communication Service on this interface? [N]

Do you want to enable HTTP on this interface? [Y]
Which port do you want to use for HTTP? [80]>

Do you want to enable HTTPS on this interface? [Y]>

Which port do you want to use for HTTPS? [443]>

Do you want to enable Spam Quarantine HTTP on this interface? [N]>

Do you want to enable Spam Quarantine HTTPS on this interface? [N]>

Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [N]>

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]>

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.

nnlookup

Description

Use the nnlookup command to check the DNS functionality.

The nnlookup command can confirm that the appliance is able to reach and resolve hostnames and IP addresses from a working DNS (domain name service) server.

<table>
<thead>
<tr>
<th>Table 3-10 nnlookup Command Query Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Type</td>
</tr>
<tr>
<td>A</td>
</tr>
<tr>
<td>CNAME</td>
</tr>
<tr>
<td>MX</td>
</tr>
</tbody>
</table>


**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.
[1]> 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’.

---

**Table 3-10 nslookup Command Query Types**

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS</td>
<td>the name server for the named zone</td>
</tr>
<tr>
<td>PTR</td>
<td>the hostname if the query is an Internet address, otherwise the pointer to other information</td>
</tr>
<tr>
<td>SOA</td>
<td>the domain’s “start-of-authority” information</td>
</tr>
<tr>
<td>TXT</td>
<td>the text information</td>
</tr>
</tbody>
</table>
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]> y
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)
```
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)
The `ping` command allows you to test connectivity to a network host from the appliance.

**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> 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=0.118 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
```

---

The `ping` command allows you to test connectivity to a network host from the appliance.

**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> 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=0.118 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
```

---

The `ping` command allows you to test connectivity to a network host from the appliance.

**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> 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=0.118 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
```
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.
[1]> anotherhost.example.com

Press Ctrl-C to stop.

Note

You must use Control-C to end the ping 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::<
• 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:

```
routenconfig new 4|6 <name> <destination_address> <gateway_ip>
```

Table 3-11 routenconfig Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>name</td>
<td>The name of the route.</td>
</tr>
<tr>
<td>destination_address</td>
<td>The IP or CIDR address to match on for outgoing IP traffic.</td>
</tr>
<tr>
<td>gateway_ip</td>
<td>The IP address to send this traffic to.</td>
</tr>
</tbody>
</table>

• Editing a static route:

```
routenconfig edit 4|6 <name> <new_name> <destination_address> <gateway_ip>
```

• Deleting a static route:

```
routenconfig 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.
[1]> new

Please create a name for the route:
[1]> EuropeNet

Please enter the destination IPv4 address to match on. CIDR addresses such as 192.168.42.0/24 are also allowed.
[1]> 192.168.12.0/24

Please enter the gateway IP address for traffic to 192.168.12.0/24:

Currently configured routes:

Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[1]>

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.

Please enter the gateway IP address for traffic to 2620:101:2004:4202::/6:
[>] 2620:101:2004:4202::23

Currently configured routes:

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 Security appliance. 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>

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

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.

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 appliance.

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: sslv3tlsv1
  GUI HTTPS ciphers:
   RC4-SHA
   RC4-MD5
   ALL
  Inbound SMTP method: sslv3tlsv1
  Inbound SMTP ciphers:
   RC4-SHA
   RC4-MD5
   ALL
  Outbound SMTP method: sslv3tlsv1
  Outbound SMTP ciphers:
   RC4-SHA
   RC4-MD5
   ALL
Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.

[]> gui

Enter the GUI HTTPS ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 6

Enter the GUI HTTPS ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
  GUI HTTPS method: sslv2sslv3tlsv1
  GUI HTTPS ciphers:
    RC4-SHA
    RC4-MD5
    ALL
  Inbound SMTP method: sslv3tlsv1
  Inbound SMTP ciphers:
    RC4-SHA
    RC4-MD5
    ALL
  Outbound SMTP method: sslv3tlsv1
  Outbound SMTP ciphers:
    RC4-SHA
    RC4-MD5
    ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.

[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 6

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]>

sslconfig settings:
  GUI HTTPS method: sslv2sslv3tlsv1
  GUI HTTPS ciphers:
    RC4-SHA
    RC4-MD5
    ALL
  Inbound SMTP method: sslv2sslv3tlsv1
  Inbound SMTP ciphers:
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.

[>] sserv3config

**Description**

Enable or disable SSLv3 settings for the appliance.

**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 how to disable SSLv3 for End User Quarantine.

```
mail.example.com> sserv3config

Current SSLv3 Settings:
----------------------------------------
  UPDATER     :     Enabled
  WEBSECURITY :     Enabled
  EUQ         :     Enabled
  LDAP        :     Enabled
----------------------------------------

Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.

[>] setup

Choose the service to toggle SSLv3 settings:
1. EUQ Service
2. LDAP Service
3. Updater Service
4. Web Security Service

[1]> Do you want to enable SSLv3 for EUQ Service ? [Y]>n
```
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.

```
[]>
```

**telnet**

**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 appliance 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.
[1]> 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 appliance 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.
[1]> example.com
Press Ctrl-C to stop.
connect: No route to host
vm10esa0031.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.
[1]> 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
Outbreak Filters

This section contains the following CLI commands:

- `outbreakconfig`
- `outbreakflush`
- `outbreakstatus`
- `outbreakupdate`

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
- Enable Logging of 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 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?
```
Do you want to use adaptive rules to compute the threat level of messages? [Y]>
Logging of URLs is currently disabled.
Do you wish to enable logging of URL's? [N] Y
Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system. You must use the 'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing Mail Policies.

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]>

outbreakflush

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

```bash
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
```

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
- exceptionconfig
- filters
- policyconfig
- quarantineconfig
- scanconfig
- stripheaders
- textconfig

**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.

[]> new

Enter a name for this content dictionary.
[]> HRWords

Do you wish to specify a file for import? [N]>

Enter new words or regular expressions, enter a blank line to finish.
<list of words typed here>

Currently configured content dictionaries:
1. HRWords

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.

[]> delete

Enter the number of the dictionary you want to delete:
1. HRWords

[]> 1

Content dictionary "HRWords" deleted.
No content dictionaries have been defined.

Choose the operation you want to perform:
- NEW - Create a new content dictionary.

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.

[]> new

Enter a name for this content dictionary.
[]> secret_words

Do you wish to specify a file for import? [N]>

Enter new words or regular expressions, enter a blank line to finish.
```
codename

Currently configured content dictionaries:
1. secret_words

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[] > **edit**
Enter the number of the dictionary you want to edit:
1. secret_words
[] > 1

Choose the operation you want to perform on dictionary 'secret_words':
- **NEW** - Create new entries in this dictionary.
- **IMPORT** - Replace all of the words in this dictionary.
- **EXPORT** - Export the words in this dictionary.
- **DELETE** - Remove an entry in this dictionary.
- **PRINT** - List the entries in this dictionary.
- **SETTINGS** - Change settings for this dictionary.

[] > **settings**

Do you want to ignore case when matching using this dictionary? [Y]

Do you want strings in this dictionary to only match complete words? [Y]

Enter the default encoding to be used for exporting this dictionary:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
11. Japanese (Shift-JIS (X0123))
13. Japanese (EUC)
[] > 2

Choose the operation you want to perform on dictionary 'secret_words':
- **NEW** - Create new entries in this dictionary.
- **IMPORT** - Replace all of the words in this dictionary.
- **EXPORT** - Export the words in this dictionary.
- **DELETE** - Remove an entry in this dictionary.
- **PRINT** - List the entries in this dictionary.
- **SETTINGS** - Change settings for this dictionary.

[]>

Currently configured content dictionaries:
1. secret_words

Choose the operation you want to perform:
- **NEW** - Create a new content dictionary.
- **EDIT** - Modify a content dictionary.
- **DELETE** - Remove a content dictionary.
- **RENAME** - Change the name of a content dictionary.

[]>

mail3.example.com > **commit**

Please enter some comments describing your changes:
[] > **Added new dictionary: secret_words**

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

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.

[>] 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)
11. Japanese (Shift-JIS (X0123))
13. Japanese (EUC)


Currently configured content dictionaries:
1. profanity

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
```

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.
- RENAME - Change the name of a content dictionary.
```
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@zzzaaazzz.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, page 3-195
- Creating a Policy for the Sales Team, page 3-197
- Creating a Policy for the Engineering Team, page 3-199
- Creating the scan_for_confidential Content Filter, page 3-201
- Creating the no_mp3s and ex_employee Content Filters, page 3-205
- Enabling Content Filters for Specific Policies, page 3-210
- DLP Policies for Default Outgoing Policy, page 3-213
- Create an Incoming Policy to Drop the Messages Identified as Bulk Email or Social Network Email, page 3-215
Creating an Incoming Mail Policy to Drop Spam Messages and Archive Suspected Spam Messages

In this example, the `policyconfig -> edit -> antispam` 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 Graymail: Content Outbreak
----- --------- --------- --------- --------- ------- ------- ------- -------
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

```
[1]> edit
```

```
Name: Anti-Spam: Anti-Virus: Advanced Graymail: Content Outbreak
----- --------- --------- --------- --------- ------- ------- ------- -------
1. DEFAULT Ironport Mcafee N/A N/A N/A Off Off Enabled
```

```
Enter the name or number of the entry you wish to edit:
[1]> 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

\[> \text{antispm}\]

Choose the operation you want to perform:
- EDIT - Edit Anti-Spam policy
- DISABLE - Disable Anti-Spam policy (Disables all policy-related actions)
\[> \text{edit}\]

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?
\[> 90\]

1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE

What do you want to do with messages identified as spam?
\[> 2\]

Do you want to archive messages identified as spam? [N]> y

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?
\[> 50\]

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?
\[> 4\]

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?
\[> 1\]

What text do you want to prepend to the subject?
\[ ([SUSPECTED SPAM] )> \text{[quarantined: possible spam]}\]

Do you want to add a custom header to messages identified as SUSPECTED spam? [N]> y

Enter the name of the header:
\[> \text{x-quarantined}\]

Enter the text for the content of the header:
\[> \text{true}\]

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

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

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

Enter the name for this policy:
sales_team

Begin entering policy members. The following types of entries are allowed:
Username entries such as joe@, domain entries such as @example.com, sub-domain entries such as .example.com, LDAP group memberships such as ldap(Engineers)

Enter a member for this policy:
[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
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced</th>
<th>Graymail: Malware</th>
<th>Protection:</th>
<th>Content Filter:</th>
<th>Outbreak Filters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>sales_team</td>
<td>IronPort</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
<td>Off</td>
<td>Enabled</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>Ironport</td>
<td>Mcafee</td>
<td>N/A</td>
<td>Off</td>
<td>Off</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced</th>
<th>Graymail: Malware</th>
<th>Protection:</th>
<th>Content Filter:</th>
<th>Outbreak Filters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>sales_team</td>
<td>IronPort</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>N/A</td>
<td>Off</td>
<td>Enabled</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>Ironport</td>
<td>Mcafee</td>
<td>N/A</td>
<td>Off</td>
<td>Off</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

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:
Policy Enforcement

Chapter 3      The Commands: Reference Examples

[1]> 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
[1]> 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
[1]> 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

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

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
Policy Enforcement

Chapter 3      The Commands: Reference Examples

[>] 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:
[ ]> [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

[1]> 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

[1]> save

Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
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

[1]> save

Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter

[1]> new

Enter a name for this filter:

[]> 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
\[> \textbf{add} \]

1. Condition
2. Action

\[1> \textbf{1} \]

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

\[1> \textbf{13} \]

Enter regular expression to search Recipient address for:

\[> \textbf{doug} \]

Filter Name: \textit{ex_employee} \n
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

\[> \textbf{add} \]

1. Condition
2. Action

\[1> \textbf{2} \]

1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check

[1]> 2

Enter the email address(es) to send the notification to:
[1]> joe@example.com

Do you want to edit the subject line used on the notification? [N]> y

Enter the subject to use:
[1]> 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

[1]> add

1. Condition
2. Action

[1]> 2

1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check

[1]> 18

Filter Name: ex_employee

Conditions:
rcpt-to == "doug"

Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of example.com")
bounce()

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter

[]> save

Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments
3. ex_employee: bounce messages intended for Doug

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter

[]>

Incoming Mail Policy Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced Malware</th>
<th>Graymail</th>
<th>Content Filter</th>
<th>Outbreak Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>sales_team</td>
<td>IronPort</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>engineering</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>Ironport</td>
<td>Mcafee</td>
<td>N/A</td>
<td>Off</td>
<td>Off</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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

Code Example illustrates how to enable the policies once again to enable the content filters for some policies, but not for others.

Incoming Mail Policy Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced</th>
<th>Graymail</th>
<th>Content Filter</th>
<th>Outbreak Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>sales_team</td>
<td>IronPort</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>engineering</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>Ironport</td>
<td>Mcafee</td>
<td>N/A</td>
<td>Off</td>
<td>Off</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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

Enter the name or number of the entry you wish to edit:

1. sales_team IronPort Default Default Default Default
2. engineering Default Default Default Default Enabled
3. DEFAULT Ironport Mcafee N/A Off Off Enabled

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.
Policy Enforcement

- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify 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:

- Name: sales_team  Anti-Spam: IronPort  Anti-Virus: Default  Advanced: Default  Graymail: Default  Content Filter: Default  Outbreak Filters: Default
- Name: engineering  Anti-Spam: Default  Anti-Virus: Default  Advanced: Default  Graymail: Default  Content Filter: Default  Outbreak Filters: Enabled
- Name: DEFAULT  Anti-Spam: Ironport  Anti-Virus: Mcafee  Advanced: N/A  Graymail: Off  Content Filter: Enabled  Outbreak Filters: Enabled

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: sales_team  Anti-Spam: IronPort  Anti-Virus: Default  Advanced: Default  Graymail: Default  Content Filter: Default  Outbreak Filters: Default

Name: engineering  Anti-Spam: Default  Anti-Virus: Default  Advanced: Default  Graymail: Default  Content Filter: Default  Outbreak Filters: Enabled

Name: DEFAULT  Anti-Spam: Ironport  Anti-Virus: Mcafee  Advanced: N/A  Graymail: Off  Content Filter: Enabled  Outbreak Filters: 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

\[
\text{\texttt{[\>] \texttt{edit}}}
\]

Enter the name or number of the entry you wish to edit:
\[
\text{\texttt{[\>] 2}}
\]

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
- ANTIISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters

\[
\text{\texttt{[\>] \texttt{filters}}}
\]

Choose the operation you want to perform:
- DISABLE - Disable Content Filters policy (Disables all policy-related actions)
- ENABLE - Enable Content Filters policy

\[
\text{\texttt{[\>] \texttt{enable}}}
\]

1. scan_for_confidential
2. no_mp3s
3. ex_employee

Enter the filter to toggle on/off, or press enter to finish:
\[
\text{\texttt{[\>] 1}}
\]

1. Active scan_for_confidential
2. no_mp3s
3. ex_employee

Enter the filter to toggle on/off, or press enter to finish:
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced Malware Protection</th>
<th>Graymail</th>
<th>Content Filter:</th>
<th>Outbreak Filters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>sales_team</td>
<td>IronPort</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>engineering</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>Ironport</td>
<td>Mcafee</td>
<td>N/A</td>
<td>Off</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

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

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

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> edit

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

1> dlp

Choose the operation you want to perform:
- ENABLE - Enable DLP policy

1> 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

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:

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:

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 Graymail: Content Outbreak
------- ----------- ----------- -------------- ------- ------- -------
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
[1]> edit
Policy Enforcement

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:
- ANTI SPAM - 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]> y

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]> y

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

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:

<table>
<thead>
<tr>
<th>#</th>
<th>Quarantine Name</th>
<th>Size (MB)</th>
<th>% full</th>
<th>Messages</th>
<th>Retention</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Outbreak</td>
<td>3,072</td>
<td>0.0</td>
<td>1</td>
<td>12h</td>
<td>Release</td>
</tr>
<tr>
<td>2</td>
<td>Policy</td>
<td>1,024</td>
<td>0.1</td>
<td>497</td>
<td>10d</td>
<td>Delete</td>
</tr>
<tr>
<td>3</td>
<td>Virus</td>
<td>2,048</td>
<td>empty</td>
<td>0</td>
<td>30d</td>
<td>Delete</td>
</tr>
</tbody>
</table>

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.

[1]> new

Please enter the name for this quarantine:

[1]> HRQuarantine

Retention period for this quarantine. (Use 'd' for days or 'h' for hours.):

[1]> 15 d

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:

<table>
<thead>
<tr>
<th>#</th>
<th>Quarantine Name</th>
<th>Size (MB)</th>
<th>% full</th>
<th>Messages</th>
<th>Retention</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HRQuarantine</td>
<td>1,024</td>
<td>N/A</td>
<td>N/A</td>
<td>15d</td>
<td>Release</td>
</tr>
<tr>
<td>2</td>
<td>Outbreak</td>
<td>3,072</td>
<td>0.0</td>
<td>1</td>
<td>12h</td>
<td>Release</td>
</tr>
<tr>
<td>3</td>
<td>Policy</td>
<td>1,024</td>
<td>0.1</td>
<td>497</td>
<td>10d</td>
<td>Delete</td>
</tr>
<tr>
<td>4</td>
<td>Virus</td>
<td>2,048</td>
<td>empty</td>
<td>0</td>
<td>30d</td>
<td>Delete</td>
</tr>
</tbody>
</table>

(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.

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 RSA Email 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
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

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)
11. Japanese (Shift-JIS (X0123))
13. Japanese (EUC)

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/*

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)
11. Japanese (Shift-JIS (X0123))
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.

[1]> 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.

[1]>

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 appliance.
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.

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
[]> import

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 ]
[]>

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 appliance.

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
- displayalerts
- findevent
- grep
- logconfig
- rollovernow
- snmpconfig
- tail
**alertconfig**

**Description**

Configure email alerts.

**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 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.

```
vm30esa0086.ibqa> alertconfig
Not sending alerts (no configured addresses)
Alerts will be sent using the system-default From Address.
Cisco IronPort AutoSupport: Disabled
Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> new
Please enter a new email address to send alerts.
(Ex: "administrator@example.com")
[]> alertadmin@example.com
Choose the Alert Classes. Separate multiple choices with commas.
1. All
2. System
3. Hardware
4. Updater
5. Outbreak Filters
6. Anti-Virus
7. Anti-Spam
8. Directory Harvest Attack Prevention
9. Release and Support Notifications
[1]> 2,3,8
Select a Severity Level. Separate multiple choices with commas.
1. All
2. Critical
3. Warning
4. Information
[1]> 2
Sending alerts to:
alertadmin@example.com
Class: Hardware - Severities: Critical
```
### displayalerts

**Description**

Display the last n alerts sent by the appliance

**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**

```plaintext
> 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.

```
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


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.
[1]> *

Currently configured logs:

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Log Type</th>
<th>Retrieval</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail_logs</td>
<td>IronPort Text Mail Logs</td>
<td>Manual Download</td>
<td>None</td>
</tr>
</tbody>
</table>

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]> 1

Currently configured logs:
<table>
<thead>
<tr>
<th>Log Name</th>
<th>Log Type</th>
<th>Retrieval</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail_logs</td>
<td>IronPort Text Mail Logs</td>
<td>Manual Download</td>
<td>None</td>
</tr>
</tbody>
</table>

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

No matching message IDs were found
```

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:
<table>
<thead>
<tr>
<th>Log Name</th>
<th>Log Type</th>
<th>Retrieval</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail_logs</td>
<td>IronPort Text Mail Logs</td>
<td>Manual Download</td>
<td>None</td>
</tr>
</tbody>
</table>

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

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 3-12  grep Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-C</td>
<td>Provides lines of context around the grep pattern found. Enter a value to specify the number of lines to include.</td>
</tr>
<tr>
<td>-e</td>
<td>Enter a regular expression.</td>
</tr>
<tr>
<td>-i</td>
<td>Ignores case sensitivities.</td>
</tr>
<tr>
<td>-p</td>
<td>Paginates the output.</td>
</tr>
<tr>
<td>-t</td>
<td>Runs the grep command over the tail of the log file.</td>
</tr>
<tr>
<td>regex</td>
<td>Enter a regular expression.</td>
</tr>
</tbody>
</table>

**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 22:47:42 2006 Info: sophos antivirus - MID 18 - Result 'VIRAL' ()
Fri Jun  9 22:53:04 2006 Info: sophos antivirus - MID 16 - Result 'VIRAL' ()
Fri Jun  9 22:53:05 2006 Info: sophos antivirus - MID 19 - Result 'VIRAL' ()
Fri Jun  9 22:53:06 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' ()
```

**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`.

```
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
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. "eug_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "eugui_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. "smtpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status 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

Password for youruser:

[>] thepassword

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
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. "eug_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. "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
20. "sntpd_logs" Type: "NTP 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 Email Security Appliances.) 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
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. "smtpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.

[?] > new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
```
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs

[1]> 3

Please enter the name for the log:

[*]> LogPush

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push

[1]> 3

Hostname to deliver the logs:

[*]> 10.1.1.1

Port to connect to on the remote host:

[22]> [22]

Username on the remote host:

[*]> logger

Directory on remote host to place logs:

[*]> /tmp

Filename to use for log files:

delivery.log>

Maximum time to wait before transferring:

[3600]>

Maximum filesize before transferring:

[10485760]>

Protocol:
1. SSH1
2. SSH2

[2]> 2

Do you want to enable host key checking?  [N]> y

Do you want to automatically scan the host for its SSH key, or enter it manually?
1. Automatically scan.
2. Enter manually.

[1]> 1
SSH2:dsa
10.1.1.1 ssh-dss
AAAAB3NzaC1kc3MAAAAACBALwGidI1WLVDn9IwEsAm9tLVE2tsE9JBf4gwLvoqG3FRqifrce92zygHtC/ZWyXav
UTl1M3d1bpiEcsceMo2XKpSbPp2y1y8bqkpJscScQcMe8z3MDjPnOFm8ghVhxYHi7oNwEJCCPnPAXy441J5Yxx9eToAL
p0dHU0GR+j1NAAAFQDQ1S0Y/X9PlDMfPMVEx7wcoedlwAAAIB9cgMTEFF1WTAG0rl1RtbwZP5zWxLVX7tldXzjlo
4+b404BR7Dkuc80-naApnTJyH/J8R3wJVF795MgeKJbxxZjGDK3ZxJy13YefPqBqXp2O12zLRQ5JSy1WXwYz/rooqN
1BnF4sh1zmtq3tdei176bqgtwQA4wKO15k3z0NsPwAAAALcRYat3y+B1v/V6w6E6BBKk+oULv3eK3qafup4WMBX
kg9Go6EQ18nss82oznWBy/p1TRqfh4Mhm1XTF4VEY0uAFsaRa12uUJC1QGQVCGh7N3YNAias2CSbEKEBa1TF6+SXZ
RNpcUF3mg9gw92xtqQPKeC2eLtK2ZJRkhC+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 AAAAB3NzaC1kc3MAAAAACBALwGidI1WLVDn9IwEsAm9tLVE2tsE9JBf4gwLvoqG3FRqifrce92zygHtC/ZWyXav
UTl1M3d1bpiEcsceMo2XKpSbPp2y1y8bqkpJscScQcMe8z3MDjPnOFm8ghVhxYHi7oNwEJCCPnPAXy441J5Yxx9eToAL
p0dHU0GR+j1NAAAFQDQ1S0Y/X9PlDMfPMVEx7wcoedlwAAAIB9cgMTEFF1WTAG0rl1RtbwZP5zWxLVX7tldXzjlo
4+b404BR7Dkuc80-naApnTJyH/J8R3wJVF795MgeKJbxxZjGDK3ZxJy13YefPqBqXp2O12zLRQ5JSy1WXwYz/rooqN
1BnF4sh1zmtq3tdei176bqgtwQA4wKO15k3z0NsPwAAAALcRYat3y+B1v/V6w6E6BBKk+oULv3eK3qafup4WMBX
kg9Go6EQ18nss82oznWBy/p1TRqfh4Mhm1XTF4VEY0uAFsaRa12uUJC1QGQVCGh7N3YNAias2CSbEKEBa1TF6+SXZ
RNpcUF3mg9gw92xtqQPKeC2eLtK2ZJRkhC+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]>
Do you want to enable host key checking? [N]> y
Currently installed host keys:
Choose the operation you want to perform:
- NEW - Add a new key.
- SCAN - Automatically download a host key.
- HOST - Display this machine's host keys.
[>] scan
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>
SSH1:rsa
10.1.1.1 1024 35
12260642076447444117847407996206675325...3520565607
6278292803379315222644864951413162182782144539869316125082823220808815740072109975632356478
5321288161878068307463282324327778100113128176672666244511191783747965898000855947022484692
079466697707373948871554575173520565607
Example of Syslog Push Log Subscription

In the following example, the `logconfig` command is used to configure a new delivery log called `MailLogSyslogPush`. The log is configured to be pushed to a remote syslog server with the IP address of 10.1.1.2, using UPD, with a 'mail' facility and stored in the directory.

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

Currently configured logs:
1. "antispm" 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
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. "eug_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "eugui_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. "snmpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status 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:

[1]> **MailLogSyslogPush**

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace

[3]> 2

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push

[1]> 4

Hostname to deliver the logs:

[1]> **10.1.1.2**

Which protocol do you want to use to transfer the log data?
1. UDP
2. TCP

[1]> 1

Which facility do you want the log data to be sent as?
1. auth
2. authpriv
3. console
4. daemon
5. ftp
6. local0
7. local1
8. local2
9. local3
10. local4
11. local5
12. local6
13. local7
14. mail
15. ntp
16. security
17. user

[14]> 14

Currently configured logs:
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
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. "eug_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "eugui_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. "snmpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status 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.

```
mail3.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.

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

Do you want to enable SNMP? [N]> y

Please choose an IP interface for SNMP requests.
1. Data 1 (192.168.1.1/24: buttercup.run)
2. Data 2 (192.168.2.1/24: buttercup.run)
3. Management (192.168.44.44/24: buttercup.run)
[1]> Enter the SNMPv3 passphrase.
> 
Please enter the SNMPv3 passphrase again to confirm.
>
Which port shall the SNMP daemon listen on?
[161]>

Service SNMP V1/V2c requests? [N]> y

Enter the SNMP V1/V2c community string.
[1]> public

From which network shall SNMP V1/V2c requests be allowed?
[192.168.2.0/24]>

Enter the Trap target (IP address). Enter "None" to disable traps.
[None]> snmp-monitor.example.com

Enterprise Trap Status
1. RAIDStatusChange Enabled
2. fanFailure Enabled
3. highTemperature Enabled
4. keyExpiration Enabled
5. linkDown Enabled
6. linkUp Enabled
7. powerSupplyStatusChange Enabled
8. resourceConservationMode Enabled
9. updateFailure Enabled

Do you want to change any of these settings? [N]> y
```
Do you want to disable any of these traps? [Y]>

Enter number or numbers of traps to disable. Separate multiple numbers with commas.
[>] 1,8

Enterprise Trap Status
1. RAIDStatusChange Disabled
2. fanFailure Enabled
3. highTemperature Enabled
4. keyExpiration Enabled
5. linkDown Enabled
6. linkUp Enabled
7. powerSupplyStatusChange Enabled
8. resourceConservationMode Disabled
9. updateFailure Enabled

Do you want to change any of these settings? [N]>

Enter the System Location string.
[Unknown: Not Yet Configured] > Network Operations Center - west; rack #31, position 2

Enter the System Contact string.
[snmp@localhost] > Joe Administrator, x8888

Current SNMP settings:
Listening on interface "Data 1" 192.168.2.1/24 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.
SNMP v1/v2 Community String: public
Trap target: snmp-monitor.example.com
Location: Network Operations Center - west; rack #31, position 2
System Contact: Joe Administrator, x8888

mail3.example.com> tail

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
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
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.
Sun May 16 00:00:00 2008 Info: Generated report: name b, start time Sun May 16 00:00:00 2004, size 2154 bytes

---

**Reporting**

This section contains the following CLI commands:
- `reportingconfig`
reportingconfig

Using the reportingconfig command

The following subcommands are available within the reportingconfig submenu:

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>filters</td>
<td>Configure filters for the Security Management appliance.</td>
<td>M-Series only</td>
</tr>
<tr>
<td>alert_timeout</td>
<td>Configure when you will be alerted due to failing to get reporting data.</td>
<td>M-Series only</td>
</tr>
<tr>
<td>domain</td>
<td>Configure domain report settings.</td>
<td>M-Series only</td>
</tr>
<tr>
<td>mode</td>
<td>Enable centralized reporting on the Security Management appliance.</td>
<td>C-, M-Series</td>
</tr>
<tr>
<td>mailsetup</td>
<td>Configure reporting for the Email Security appliance.</td>
<td>C-Series only</td>
</tr>
</tbody>
</table>

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
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.
[]>

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 Security Appliance

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.

[>]

Senderbase

This section contains the following CLI commands:

- sbstatus
- senderbaseconfig

sbstatus

Description

Display status of SenderBase queries.

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> sbstatus
SenderBase host status
Status as of: Tue Oct 21 10:55:04 2003
Host up/down: up

If the appliance is unable to contact the SenderBase Reputation Service, or the service has never been contacted, the following is displayed:

mail3.example.com> sbstatus
SenderBase host status
Host up/down: Unknown (never contacted)
senderbaseconfig

Description

Configure SenderBase connection 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> senderbaseconfig

Share statistics with SenderBase Information Service: Enabled

Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings

[>] setup

Do you want to share statistical data with the SenderBase Information Service (recommended)? [Y]>

Share statistics with SenderBase Information Service: Enabled

Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings

[>]
```

SMTP Services Configuration

This section contains the following CLI commands:

- callaheadconfig
- listenerconfig
- localeconfig
- smtpauthconfig
- smtpauthconfig

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
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
- Validation Failure Action: ACCEPT
- Temporary Failure Action: REJECT with same code
- Maximum number of connections: 5
- Maximum number of validation queries: 1000
- Cache size: 10000
- Cache TTL: 900

Do you want to change advanced settings? [N]> n

Currently configured SMTP Call-Ahead profiles:
1. Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)

Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.

[>] print

Select the profile you want to print:
1. Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)
[1]>

**listenerconfig**

**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 appliance communicates with the system that is injecting email.

## Table 3-14 listenerconfig Commands

<table>
<thead>
<tr>
<th>Name</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Interface</td>
<td>Listeners are assigned to IP interfaces. All IP interfaces must be configured using the systemstartup command or the interfaceconfig command before you create and assign a listener to it.</td>
</tr>
<tr>
<td>Mail protocol</td>
<td>The mail protocol is used for email receiving: either ESMTP or QMOP</td>
</tr>
<tr>
<td>IP Port</td>
<td>The specific IP port used for connections to the listener. by default SMTP uses port 25 and QMOP uses port 628.</td>
</tr>
<tr>
<td>Listener Type:</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Blackhole “Blackhole” listeners can be used for testing or troubleshooting purposes. When you create a blackhole listener, you choose whether messages are written to disk or not before they are deleted. (See the “Testing and Troubleshooting” chapter of the User Guide for AsyncOS for Cisco Email Security Appliances for more information.)</td>
</tr>
</tbody>
</table>

### 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.
SMTP Services Configuration

Chapter 3      The Commands: Reference Examples

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 3-15, “listenerconfig Argument Values -HAT,” on page 252

- Adding a new listener:

  ```
  listenerconfig new <name> <public|private|blackhole|blackholequeueing> <interface_name> <smtp|qmqp>
  ```

- Deleting a listener:

  ```
  listenerconfig delete <name>
  ```

- 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 sendergroup <name> hostaccess edit sendergroup <name> new <host_list>
  ```

- Delete a host from a sendergroup

  ```
  listenerconfig edit sendergroup <name> hostaccess edit sendergroup <name> delete <host>
  ```

- Move a host in a sendergroup’s list order

  ```
  listenerconfig edit sendergroup <name> hostaccess edit sendergroup <name> move <host> <host-to-insert-before>
  ```

- Modify a sendergroup’s policy

  ```
  listenerconfig edit sendergroup <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 sendergroup <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 appliance
  
  ```
  listenerconfig edit <name> hostaccess export <filename>
  ```

- Deleting all user defined sendergroups and policies from the HAT
  
  ```
  listenerconfig edit <name> hostaccess clear
  ```
### Table 3-15  
**listenerconfig Argument Values -HAT**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;behavior&gt;</code></td>
<td>“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).</td>
</tr>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The filename to use with importing and exporting the hostaccess tables.</td>
</tr>
<tr>
<td><code>&lt;group&gt;</code></td>
<td>A sendergroup <code>&lt;name&gt;</code>.</td>
</tr>
</tbody>
</table>
| `<host>` | A single entity of a `<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 blacklist queries (dnslist[query.blacklist.example] |
| `<host_list>` | 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. |
| `<name>` | Note: Separate multiple hosts with commas |


### Table 3-15  
listenerconfig Argument Values -HAT

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--max_size</td>
<td>Maximum message size. Add a trailing k for kilobytes, M for megabytes, or no letters for bytes.</td>
</tr>
<tr>
<td>--max_conn</td>
<td>Maximum number of connections allowed from a single host.</td>
</tr>
<tr>
<td>--max_msgs</td>
<td>Maximum number of messages per connection.</td>
</tr>
<tr>
<td>--max_rcpt</td>
<td>Maximum number of recipients per message.</td>
</tr>
<tr>
<td>--override</td>
<td>Override the hostname in the SMTP banner. “No” or SMTP banner string.</td>
</tr>
<tr>
<td>--cust_acc</td>
<td>Specify a custom SMTP acceptance response. “No” or SMTP acceptance response string.</td>
</tr>
<tr>
<td>--acc_code</td>
<td>Custom SMTP acceptance response code. Default is 220.</td>
</tr>
<tr>
<td>--cust_rej</td>
<td>Specify a custom SMTP rejection response. “No” or SMTP rejection response string.</td>
</tr>
<tr>
<td>--rej_code</td>
<td>Custom SMTP rejection response code. Default is 554.</td>
</tr>
<tr>
<td>--rate_lim</td>
<td>Enable rate limiting per host. “No”, “default” or maximum number of recipients per hour per host.</td>
</tr>
<tr>
<td>--cust_lim</td>
<td>Specify a custom SMTP limit exceeded response message. “No” or SMTP rejection response string. Default is “No”.</td>
</tr>
<tr>
<td>--lim_code</td>
<td>Custom SMTP limit exceeded response code. Default is 452.</td>
</tr>
<tr>
<td>--use_sb</td>
<td>Use SenderBase for flow control by default. “Yes”, “No”, or “default”.</td>
</tr>
<tr>
<td>--as_scan</td>
<td>Enable anti-spam scanning. “Yes”, “No”, “Default”.</td>
</tr>
<tr>
<td>--av_scan</td>
<td>Enable anti-virus scanning. “Yes”, “No”, “Default”.</td>
</tr>
<tr>
<td>--dhap</td>
<td>Directory Harvest Attack Prevention. “No”, “default”, or maximum number of invalid recipients per hour from a remote host.</td>
</tr>
<tr>
<td>--tls</td>
<td>Not supported; use menuing system to configure TLS.</td>
</tr>
<tr>
<td>--sig_bits</td>
<td>Number of bits of IP address to treat as significant. From 0 to 32, “No” or “default”.</td>
</tr>
<tr>
<td>--dkim_verification</td>
<td>Enable DKIM verification. “Yes”, “No”, “Default.”</td>
</tr>
<tr>
<td>--dkim_verification_profile &lt;name&gt;</td>
<td>The name of DKIM verification profile. This option is only applicable if --dkim_verification value is set to “Yes.”</td>
</tr>
</tbody>
</table>
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 3-16, “listenerconfig Argument Values - RAT,” on page 255.

- Adding a new recipient to the RAT

  \[ \text{listenerconfig edit <name> rcptaccess new <rat_addr> [options]} \]

- Editing a recipient in the RAT

  \[ \text{listenerconfig edit <name> rcptaccess edit <rat_addr> [options]} \]

- Deleting a recipient from the RAT

  \[ \text{listenerconfig edit <name> rcptaccess delete <rat_addr>} \]

- Printing a copy of the RAT

  \[ \text{listenerconfig edit <name> rcptaccess print} \]

- Importing a local RAT to your appliance

  \[ \text{listenerconfig edit <name> rcptaccess import <filename>} \]
- Exporting a RAT

```
listenerconfig edit <name> rcptaccess export <filename>
```

- Clearing the default access

```
listenerconfig edit <name> rcptaccess clear <default_access>
```

**Table 3-16 listenerconfig Argument Values - RAT**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;rat_addr&gt;</td>
<td>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 (<a href="mailto:joe@example.com">joe@example.com</a>, joe@[1.2.3.4])</td>
</tr>
<tr>
<td>&lt;options&gt;</td>
<td></td>
</tr>
<tr>
<td>--action</td>
<td>Action to apply to address(es). Either “Accept” or “Reject”. Default is “Accept”.</td>
</tr>
<tr>
<td>--cust_resp</td>
<td>Specify a custom SMTP response. “No” or SMTP acceptance response string.</td>
</tr>
<tr>
<td>--resp_code</td>
<td>Custom SMTP response code. Default is 250 for “Accept” actions, 550 for “Reject”.</td>
</tr>
<tr>
<td>--bypass_rc</td>
<td>Bypass receiving control. Default is “No”.</td>
</tr>
<tr>
<td>--bypass_la</td>
<td>Bypass LDAP Accept query. Either “Yes” or “No.”</td>
</tr>
</tbody>
</table>

**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.
```
Chapter 3      The Commands: Reference Examples

SMTP Services Configuration

- 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. Blackhole
[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.
Example - Customizing the Host Acess 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 Email Security Appliances*.

To customize a HAT for a listener you have defined via export and import:

**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`.

```
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: Disabled
Max Concurrency: 1000 (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.
- 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.
```

---

- DELETE - Remove a listener.
- SETUP - Change global settings.
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.

$BLOCKED
  REJECT {}$TRUSTED
  ACCEPT {
    tls = "off"
    dhap_limit = 0
    max_rcpts_per_hour = -1
    virus_check = "on"
    max_msgs_per_session = 5000
    spam_check = "off"
    use_sb = "off"
    max_message_size = 104857600
    max_rcpts_per_msg = 5000
    max_concurrency = 600
  }$ACCEPTED
  ACCEPT {}$THROTTLED
  ACCEPT {
    tls = "off"
    dhap_limit = 0
    max_rcpts_per_hour = 1
    virus_check = "on"
max_msgs_per_session = 10
spam_check = "on"
use_sb = "on"
max_message_size = 1048576
max_rcpts_per_msg = 25
max_concurrency = 10

WHITELIST:
   $TRUSTED (My trusted senders have no anti-spam or rate limiting)

BLACKLIST:
   $BLOCKED (Spammers are rejected)

SUSPECTLIST:
   $THROTTLED (Suspicious senders are throttled)

UNKNOWNLIST:
   $ACCEPTED (Reviewed but undecided, continue normal acceptance)

ALL
   $ACCEPTED (Everyone else)

Default Policy Parameters
==========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes

There are currently 4 policies defined.
There are currently 5 sender groups.

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

[]> export

Enter a name for the exported file:
[]> inbound.HAT.txt

File written on machine "mail3.example.com".

**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:

- The first two entries reject all connections from the remote hosts in the domain spamdomain.com and any subdomain of spamdomain.com.
- 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 Security appliance 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 Email Security Appliances.

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 Appliance,” 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.

```
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
use_sb = "on"
tls = "off"
}

$TRUSTED
ACCEPT {
spam_check = "off"
max_msgs_per_session = 5000
max_concurrency = 600
max_rcpts_per_msg = 5000
max_rcpts_per_hour = -1
dhap_limit = 0
virus_check = "on"
max_message_size = 104857600
use_sb = "off"
tls = "off"
}

$BLOCKED
REJECT

WHITELIST:
$TRUSTED (My trusted senders have no anti-spam scanning or rate limiting)

BLACKLIST:
$BLOCKED (Spammers are rejected)

SUSPECTLIST:
$THROTTLED (Suspicious senders are throttled)

UNKNOWNLIST:
$ACCEPTED (Reviewed but undecided, continue normal acceptance)

spamdomain.com
REJECT (reject the domain "spamdomain.com")

spamdomain.com
REJECT (reject all subdomains of ".spamdomain.com")
251.192.1.
    TCPREFUSE (TCPREFUSE the IP addresses in "251.192.1")

169.254.10.10
    RELAY (RELAY the address 169.254.10.10)

ALL
    $ACCEPTED (Everyone else)

Default Policy Parameters
=================================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[\]> 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  
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
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 ENS 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.
Example - Advanced HAT Parameters

Table 3-17 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 Table 3-17.

Table 3-17  Advanced HAT Parameter Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Syntax</th>
<th>Values</th>
<th>Example Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum messages per connection</td>
<td>max_msgs_per_session</td>
<td>Number</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum recipients per message</td>
<td>max_rcpts_per_msg</td>
<td>Number</td>
<td>10000</td>
</tr>
<tr>
<td>Maximum message size</td>
<td>max_message_size</td>
<td>Number</td>
<td>1048576</td>
</tr>
<tr>
<td>Maximum concurrent connections allowed to this listener</td>
<td>max_concurrency</td>
<td>Number</td>
<td>1000</td>
</tr>
<tr>
<td>SMTP Banner Code</td>
<td>smtp_banner_code</td>
<td>Number</td>
<td>220</td>
</tr>
<tr>
<td>SMTP Banner Text (*)</td>
<td>smtp_banner_text</td>
<td>String</td>
<td>Accepted</td>
</tr>
<tr>
<td>SMTP Reject Banner Code</td>
<td>smtp_banner_code</td>
<td>Number</td>
<td>550</td>
</tr>
<tr>
<td>SMTP Reject Banner Text (*)</td>
<td>smtp_banner_text</td>
<td>String</td>
<td>Rejected</td>
</tr>
<tr>
<td>Override SMTP Banner Hostname</td>
<td>use_override_hostname</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td>override_hostname</td>
<td>String</td>
<td>newhostname</td>
</tr>
<tr>
<td>Use TLS</td>
<td>tls</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>Use anti-spam scanning</td>
<td>spam_check</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>Use Sophos virus scanning</td>
<td>virus_check</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>Maximum Recipients per Hour</td>
<td>max_rcpts_per_hour</td>
<td>Number</td>
<td>5k</td>
</tr>
<tr>
<td>Maximum Recipients per Hour Error Code</td>
<td>max_rcpts_per_hour_code</td>
<td>Number</td>
<td>452</td>
</tr>
<tr>
<td>Maximum Recipients per Hour Text (*)</td>
<td>max_rcpts_per_hour_text</td>
<td>String</td>
<td>Too many recipients</td>
</tr>
<tr>
<td>Use SenderBase</td>
<td>use_sb</td>
<td>on</td>
<td>off</td>
</tr>
</tbody>
</table>
SMTP Services Configuration

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 appliance performs, based on the SPF/SIDF verification results. You can also define the SMTP response that the appliance 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 appliance 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 appliance 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 appliance 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 appliance automatically accepts all verification results, including Fail.

The appliance 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 appliance accepts that result. If the message then fails the MAIL FROM identity check, the listener terminates the session and then returns the STMP response for the REJECT action.

The SMTP response is a code number and message that the appliance 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.

---

### Table 3-17 Advanced HAT Parameter Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Syntax</th>
<th>Values</th>
<th>Example Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define SenderBase Reputation Score</td>
<td>sbrs[value1:value2]</td>
<td>-10.0 - 10.0</td>
<td>sbrs[-10:-7.5]</td>
</tr>
<tr>
<td>Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour</td>
<td>dhap_limit</td>
<td>Number</td>
<td>150</td>
</tr>
</tbody>
</table>
Optionally, you can configure the appliance 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 appliance 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 3-18 SPF Control Settings**

<table>
<thead>
<tr>
<th>Conformance Level</th>
<th>Available SPF Control Settings</th>
</tr>
</thead>
</table>
| SPF Only           | • whether to perform HELO identity check  
|                    | • SMTP actions taken based on the results of the following identity checks:  
|                    | • HELO identity (if enabled)  
|                    | • MAIL FROM Identity  
|                    | • SMTP response code and text returned for the REJECT action  
|                    | • verification time out (in seconds)  |
The following example shows a user configuring the SPF/SIDF verification using the SPF Only conformance level. The appliance 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 appliance automatically accepts all verification results for the identity. The appliance 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

### Table 3-18 SPF Control Settings

<table>
<thead>
<tr>
<th>Conformance Level</th>
<th>Available SPF Control Settings</th>
</tr>
</thead>
</table>
| SIDF Compatible     | • 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:  
|                     |   • 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          | • SMTP actions taken based on the results of the following identity checks:  
|                     |   • MAIL FROM Identity  
|                     |   • PRA Identity  
|                     |   • SMTP response code and text returned in case of SPF REJECT action  
|                     |   • verification timeout (in seconds)  |
What SMTP action should be taken if HELO check returns None?
1. Accept
2. Reject
[1]> 1

What SMTP action should be taken if HELO check returns Neutral?
1. Accept
2. Reject
[1]> 1

What SMTP action should be taken if HELO check returns SoftFail?
1. Accept
2. Reject
[1]> 2

What SMTP action should be taken if HELO check returns Fail?
1. Accept
2. Reject
[1]> 2

What SMTP action should be taken if HELO check returns TempError?
1. Accept
2. Reject
[1]> 2

What SMTP action should be taken if HELO check returns PermError?
1. Accept
2. Reject
[1]> 2

Would you like to change SMTP actions taken for the MAIL FROM identity? [N]> n

Would you like to change SMTP response settings for the REJECT action? [N]> n

Verification timeout (seconds)
[40]> 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.
- MASKERADE - 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
Chapter 3      The Commands: Reference Examples

SMTP Services Configuration

Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No

There are currently 4 policies defined.
There are currently 5 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.

[>] default

Enter the default maximum message size. Add a trailing k for kilobytes, M for megabytes, or no letter for bytes.
[20M]>

Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner? [N]>

Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>

Would you like to specify a custom SMTP DHAP response? [Y]>

Enter the SMTP code to use in the response. 550 is the standard code.
[550]>
Enter your custom SMTP response. Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default? [Y]>

Would you like to enable anti-spam scanning? [Y]>

Would you like to enable anti-virus scanning? [Y]>

Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>

Would you like to enable DKIM/DomainKeys signing? [N]> Y

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
SMTP Services Configuration

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.
SMTP Services Configuration

- 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.

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 encodings bodies and footers: Use encoding of message footer

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, 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. Imposing the encoding of the body on the header may encode the header more precisely.) [Y]>

When there is an encoding mismatch between the message body and a footer, the system initially attempts to encode the entire message in the same encoding as the message body. If the system cannot combine the message body and the footer in the same encoding, do you
want the system to failover and attempt to encode the entire message using the encoding of the message footer? (When this feature is enabled, the system will attempt to display the footer "in-line" rather than defaulting to adding it as an attachment.) [N]> y  

Behavior when modifying headers: Use encoding of message body  
Behavior for untagged non-ASCII headers: Impose encoding of message body  
**Behavior for mismatched encodings bodies and footers: Use encoding of message body**

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
[1]>

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.

**Note**
You may specify more than one forwarding server in a profile. SASL mechanisms CRAM-MD5 and DIGEST-MD5 are not supported between the Email Security appliance 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 password to a new value.
Old password:
New password:
Retype new password:

*****
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 "0xffffffff00"): [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]>

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]>

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]>

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
Chapter 3      The Commands: Reference Examples

System Setup

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.
[1]> 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.
[1]> 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 

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
- urllistconfig
- webcacheflush
- websecurityadvancedconfig
- websecurityconfig
- websecuritydiagnostics

aggregatorconfig

Description

Configure address for Cisco Aggregator Server on the Email Security appliance. 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

urllistconfig

Description

Configure or import whitelists 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

```bash
> urllistconfig
No URL lists configured.
Choose the operation you want to perform:
NEW - Create a new URL list-
[>] new
Do you want to import a URL list?
[N]> Enter a name for the URL list
[>] sample
Enter the URL domains that need to be skipped from scanning for URL Filtering.
Enter one URL domain per line and ‘.’ to finish.
cisco.com
ironport.com/*
*.example.com
10.2.4.5/24
[2001:DB8::1]
URL list sample added.
There are currently 4 URL lists configured.
Choose the operation you want to perform:
- NEW - Create a new URL whitelist.
- EDIT - Modify an existing URL whitelist.
- DELETE - Delete an existing URL whitelist.
[>] EDIT
Choose the operation to edit the URL whitelist:
- IMPORT - Import a file into an existing URL whitelist
- EXPORT - Export an existing URL whitelist into a file
- RENAME - Rename an existing URL whitelist
[>] IMPORT
Assign new name to the imported list? (By default, name stored in the file will be applied to the list)
[N] > Y
Enter name of the list > new_list
Enter filename to import from > URLfile
NOTE: These files will be stored in /pub/configuration
URL list “new_list” added.
```
webcacheflush

Description
Flush the cache used by URL filtering features. Use this command if you change the certificate that is used for communication with Cisco Web Security Services. Generally, you will use this command only at the direction of Cisco support.

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
> webcacheflush
Web Security cache has been flushed.

websecurityadvancedconfig

Description
Configure advanced settings for URL filtering.

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 is restricted to machine mode.
Batch Command: This command supports a batch format.

Batch Format
For the batch format, see the CLI inline help.

Example
> websecurityadvancedconfig
websecurityconfig

Description

Configure basic settings for URL filtering (URL reputation and URL category features.) 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 whitelist URLs using a URL list? [N]> y
1. urllist1
2. urllist2
3. No URL list
Enter the number of URL list [1]> 1
URL list 'urllist1' added

mail.example.com> websecurityconfig
URL Filtering is enabled.
URL list 'urllist1' used.
System provided certificate used.
Web Interaction Tracking is enabled.

websecuritydiagnostics

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
- password or passwd
- last
- who
- whoami

**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)

Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change password and account policy settings.
- PASSWORD - Change the password for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRAKING - Configure DLP tracking privileges.
[>] new

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 password? [N]>

Enter the password for helpdesk

[]>

Please enter the new password 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 password and account policy settings.
- PASSWORD - Change the password for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTACKING - Configure DLP tracking privileges.

This example shows how to set up a RADIUS server for external authentication. To set up a RADIUS server, enter the hostname, port, shared password, and whether to use CHAP or PAP for the authentication protocol.

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 password, and whether to use CHAP or PAP for the authentication protocol.

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 password, and whether to use CHAP or PAP for the authentication protocol.
- 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 passwords.)
[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 password:
>
Please enter the new password again:
>

Please enter timeout in seconds for receiving a valid reply from the server:
[5]> 1

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.
[]>

password or passwd

Description

Change your password.
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).

---

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

---

**Example**

```bash
mail3.example.com> password

Old password: your_old_password
New password: your_new_password
Retype new password: your_new_password
Password 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**

```bash
elroy.run> last

+----------+------------+-------------+-------------+----------+
<table>
<thead>
<tr>
<th>Username</th>
<th>Remote Host</th>
<th>Login Time</th>
<th>Logout Time</th>
<th>Total Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>10.251.23.186</td>
<td>Thu Sep 01 09:14</td>
<td>still logged in</td>
<td>1h 5m</td>
</tr>
<tr>
<td>admin</td>
<td>10.251.23.186</td>
<td>Wed Aug 31 14:00</td>
<td>Wed Aug 31 14:01</td>
<td>1m</td>
</tr>
<tr>
<td>admin</td>
<td>10.251.23.142</td>
<td>Wed Aug 31 11:26</td>
<td>Wed Aug 31 11:38</td>
<td>11m</td>
</tr>
<tr>
<td>admin</td>
<td>10.251.23.142</td>
<td>Wed Aug 31 11:05</td>
<td>Wed Aug 31 11:09</td>
<td>4m</td>
</tr>
<tr>
<td>admin</td>
<td>10.251.23.142</td>
<td>Wed Aug 31 10:52</td>
<td>Wed Aug 31 10:53</td>
<td>1m</td>
</tr>
</tbody>
</table>
```
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
```
Virtual Appliance Management

- loadlicense
- showlicense

### loadlicense

**Description**


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:
[1]> <filename>

TERMS AND CONDITIONS OF USE
<Terms and conditions>

Do you accept the above license agreement?
[1]> 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 appliance 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

compny: Example Inc.
org: Widget Division
unit: Portland Data Center
seats: 1000
city: Portland
state: Oregon
country: US
eemail: 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