IRONPORT®
SYSTEMS

IronPort AsyncOS™ 7.3

CLI REFERENCE GUIDE

for Cisco IronPort Appliances

COPYRIGHT

Part Number: OL-23407-01
Revision Date: August 12, 2010

Table of Contents

List of Command Line Interface Examples

List of Tables

Preface

The *Cisco IronPort AsyncOS 7.3 CLI Reference Guide* provides detail listings and examples for use of the AsyncOS command line interface on the IronPort Email Security appliance. These instructions are designed for an experienced system administrator with knowledge of networking and email administration.

BEFORE YOU READ THIS BOOK

This guide assumes that you have already installed and configured your IronPort appliance. You should also be familiar with the *Cisco IronPort AsyncOS Configuration Guide*, *Cisco IronPort AsyncOS Advanced Configuration Guide*, and *Cisco IronPort AsyncOS Daily Management Guide*.

Note — If you have already cabled your appliance to your network, ensure that the default IP address for the IronPort 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 to Chapter 3, "Setup and Installation," in the *Cisco IronPort AsyncOS Configuration Guide* for more information about assigning IP addresses to the IronPort appliance.

Documentation Set

The documentation for the Cisco IronPort Email Security appliance includes the following books:

- *Cisco IronPort AsyncOS for Email Daily Management Guide*. This guide provides instructions for performing common, everyday tasks that system administrators use to manage and monitor the IronPort appliance, such as viewing email traffic using the Email Security Monitor, tracking email messages, managing system quarantines, and troubleshooting the appliance. It also provides reference information for features that system administrators interact with on a regular basis, including Email Security Monitor pages, AsyncOS logs, CLI support commands, and quarantines.
- *Cisco IronPort AsyncOS for Email Configuration Guide*. This guide is recommended for system administrators who are setting up a new IronPort appliance and want to learn about its email delivery features. It provides instructions on installing the appliance into an existing network infrastructure and setting it up as an email gateway appliance. It also includes reference information and configuration instructions for email delivery features such as the Email Pipeline, Virus Outbreak Filters, content filters, email encryption, anti-virus scanning, and anti-spam scanning.
- *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*. This guide provides instructions configuring the advanced features of the IronPort appliance. Topics include configuring the appliance to work with LDAP, creating message filters to enforce email policies, organizing multiple appliances into clusters, and customizing the listeners on the

appliance. In addition to configuration, this guide provides reference material for advanced features such as message filter rules and actions, regular expressions used in content dictionaries and message filter rules, and LDAP query syntax and attributes.

- *IronPort AsyncOS CLI Reference Guide*. This guide provides a detailed list of the commands in the AsyncOS command line interface (CLI), as well as examples of the commands in use. System administrators can use this guide for reference when using the CLI on the IronPort appliance.

HOW THIS BOOK IS ORGANIZED

Chapter 1, "AsyncOS CLI Quick Reference Guide," provides a quick reference for most commands in the CLI.

Chapter 2, "Command Line Interface: The Basics," covers the basics of using the CLI: how to access the CLI, general CLI use, batch commands, and more.

Chapter 3, "The Commands: Reference Examples," provides sample CLI sessions for each command.

TYPOGRAPHIC CONVENTIONS

Typeface or Symbol	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output.	`Please choose an IP interface for this Listener.` The `sethostname` command sets the name of the IronPort appliance.
`AaBbCc123`	What you type, when contrasted with on-screen computer output.	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**
AaBbCc123	Book titles, new words or terms, words to be emphasized. Command line variable; replace with a real name or value.	Read the *IronPort QuickStart Guide*. The IronPort appliance *must* 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:` **`ironport`** `New password:` *your_new_password* `Retype new password:` *your_new_password*

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general email and web 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 Cisco and Cisco IronPort users.

You access the Cisco Support Community at the following URL:

`https://supportforums.cisco.com`

Cisco IronPort Technical Training

Cisco IronPort Systems Technical Training Services can help you acquire the knowledge and skills necessary to successfully evaluate, integrate, deploy, maintain, and support IronPort security products and solutions.

Use one of the following methods to contact Cisco IronPort Technical Training Services:

Training. For question relating to registration and general training:

- `http://training.ironport.com`

- training@ironport.com

Certifications. For questions relating to certificates and certification exams:

- http://training.ironport.com/certification.html
- certification@ironport.com

Knowledge Base

You can access the IronPort Knowledge Base on the Cisco IronPort Customer Support page at the following URL:

http://cisco.com/web/ironport/index.html

Note — You need a Cisco support account to access the site. If you do not already have an account, click the Register link on the Support page. Generally, only Cisco customers, partners, and employees can access the Support page.

The Knowledge Base contains a wealth of information on topics related to IronPort products.

Articles generally fall into one of the following categories:

- **How-To.** These articles explain how to do something with an IronPort product. For example, a how-to article might explain the procedures for backing up and restoring a database for an appliance.
- **Problem-and-Solution.** A problem-and-solution article addresses a particular error or issue that you might encounter when using an IronPort product. For example, a problem-and-solution article might explain what to do if a specific error message is displayed when you upgrade to a new version of the product.
- **Reference.** Reference articles typically provide lists of information, such as the error codes associated with a particular piece of hardware.
- **Troubleshooting.** Troubleshooting articles explain how to analyze and resolve common issues related to IronPort products. For example, a troubleshooting article might provide steps to follow if you are having problems with DNS.

Each article in the Knowledge Base has a unique answer ID number.

Cisco IronPort Customer Support

You can request Cisco IronPort product support by phone, email, or online 24 hours a day, 7 days a week.

During Customer Support hours — 24 hours a day, Monday through Friday, excluding U.S. holidays — an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of Customer Support hours, contact IronPort using one of the following methods:

U.S. Toll-free: 1 (877) 641-4766

International: http://cisco.com/web/ironport/contacts.html

Support Page: `http://cisco.com/web/ironport/index.html`

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

Third Party Contributors

Some software included within IronPort AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in IronPort license agreements.

The full text of these agreements can be found here:

`https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.`

Portions of the software within IronPort AsyncOS is based upon the RRDtool with the express written consent of Tobi Oetiker.

Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of McAfee, Inc. Portions of this document are reproduced with permission of Sophos Plc.

IronPort Welcomes Your Comments

The IronPort 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:

docfeedback@ironport.com

Please include the following part number in the subject of your message: OL-23407-01.

CHAPTER 1

AsyncOS CLI Quick Reference Guide

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

Table 1-1 CLI Commands (No `commit` required)

CLI Command	Description	Platform Availability
`antispamstatus`	Display Anti-Spam status	C- and X- Series
`antispamupdate`	Manually update spam definitions	C- and X- Series
`antivirusstatus`	Display anti-virus status	C- and X- Series
`antivirusupdate`	Manually update virus definitions	C- and X- Series
`archivemessage`	Archives older messages in your queue.	C- and X- Series
`bouncerecipients`	Bounce messages from the queue	C-, X-, and M-Series
`clearchanges or clear`	Clear changes	C-, X-, and M-Series
`commit`	Commit changes	C-, X-, and M-Series
`commitdetail`	Display detailed information about the last commit	C- and X- Series
`deleterecipients`	Delete messages from the queue	C-, X-, and M-Series
`delivernow`	Reschedule messages for immediate delivery	C-, X-, and M-Series
`diagnostic`	Check RAID disks, network caches, and SMTP connections. Clear network caches.	C-, X-, and M-Series

Table 1-1 CLI Commands (No `commit` required) (Continued)

`dnsflush`	Clear all entries from the DNS cache	C-, X-, and M-Series
`dnslistflush`	Flush the current DNS List cache	C- and X- Series
`dnslisttest`	Test a DNS lookup for a DNS-based list service	C- and X- Series
`dnsstatus`	Display DNS statistics	C-, X-, and M-Series
`encryptionstatus`	Shows the version of the PXE Engine and Domain Mappings file	C- and X-Series
`encryptionupdate`	Requests an update to the PXE Engine	C- and X-Series
`featurekey`	Administer system feature keys	C-, X-, and M-Series
`fipsconfig`	Configure FIPS settings	C-Series
`grep`	Search for text in a log file	C-, X-, and M-Series
`help or h or ?`	Help	C-, X-, and M-Series
`hostrate`	Monitor activity for a particular host	C-, X-, and M-Series
`hoststatus`	Get the status of the given hostname	C-, X-, and M-Series
`last`	Display who has recently logged into the system	C-, X-, and M-Series
`ldapflush`	Flush any cached LDAP results	C- and X- Series
`ldaptest`	Perform a single LDAP query test	C- and X- Series
`mailconfig`	Mail the current configuration to an email address	C-, X-, and M-Series
`nslookup`	Query a name server	C-, X-, and M-Series
`netstat`	Display network connections, routing tables, and network interface statistics.	C-, X-, and M-Series
`oldmessage`	displays a list of old messages in the queue.	C- and X- Series
`ping`	Ping a network host	C-, X-, and M-Series

Table 1-1 CLI Commands (No `commit` required) (Continued)

`quit or q or exit`	Quit	C-, X-, and M-Series
`rate`	Monitor message throughput	C-, X-, and M-Series
`reboot`	Restart the system	C-, X-, and M-Series
`removemessage`	Removes old, undelivered messages from your queue.	C- and X- Series
`resetconfig`	Restore the factory configuration defaults	C-, X-, and M-Series
`resetcounters`	Reset all of the counters in the system	C-, X-, and M-Series
`resume`	Resume receiving and deliveries	C-, X-, and M-Series
`resumedel`	Resume deliveries	C-, X-, and M-Series
`resumelistener`	Resume receiving	C-, X-, and M-Series
`rollovernow`	Roll over a log file	C-, X-, and M-Series
`saveconfig`	Saves the configuration to disk	C-, X-, and M-Series
`sbstatus`	Display status of SenderBase queries	C- and X- Series
`settime`	Manually set the system clock	C-, X-, and M-Series
`showmessage`	Displays old undelivered messages in your queue.	C- and X- Series
`showconfig`	Display all configuration values	C-, X-, and M-Series
`shutdown`	Shut down the system to power off	C-, X-, and M-Series
`status`	System status	C-, X-, and M-Series
`supportrequest`	Send a message to IronPort Customer Care	C-, X-, and M-Series
`suspend`	Suspend receiving and deliveries	C-, X-, and M-Series
`suspenddel`	Suspend deliveries	C-, X-, and M-Series

Table 1-1 CLI Commands (No `commit` required) (Continued)

`suspendlistener`	Suspend receiving	C-, X-, and M-Series
`systemsetup`	First time system setup	C- and X- Series
`tail`	Continuously display the end of a log file.	C-, X-, and M-Series
`techsupport`	Allow IronPort customer service to access your system	C-, X-, and M-Series
`telnet`	Connect to a remote host	C-, X-, and M-Series
`tlsverify`	Establish an outbound TLS connection to a remote host and debug any TLS connection issues	C- and X- Series
`tophosts`	Display the top hosts by queue size	C-, X-, and M-Series
`topin`	Display the top hosts by number of incoming connections	C-, X-, and M-Series
`trace`	Trace the flow of a message through the system	C-, X-, and M-Series
`traceroute`	Display the network route to a remote host	C-, X-, and M-Series
`upgrade`	Install an upgrade	C-, X-, and M-Series
`version`	View system version information	C-, X-, and M-Series
`vofflush`	Clear the cached Outbreak Rules	C- and X- Series
`vofstatus`	Display current Outbreak Rules	C- and X- Series
`vofupdate`	Update Virus Outbreak Filter rules	C- and X- Series
`who`	List who is logged in	C-, X-, and M-Series
`whoami`	Display your current user id	C-, X-, and M-Series
`workqueue`	Display and/or alter work queue pause status	C- and X- Series

The commands in Table 1-2 require you to issue the `commit` command in order to take effect

Table 1-2 CLI Commands (`commit` required)

CLI Command	Description	Platform Availability
`addressconfig`	Configure From: addresses for system generated mail	C-, X-, and M- Series
`adminaccessconfig`	Configure network access list and banner login	C- and X- Series
`alertconfig`	Configure email alerts	C-, X-, and M- Series
`aliasconfig`	Configure email aliases	C- and X- Series
`altsrchost`	Configure Virtual Gateway™ mappings	C- and X- Series
`antispamconfig`	Configure Anti-Spam policy	C- and X- Series
`antivirusconfig`	Configure anti-virus policy	C- and X- Series
`bounceconfig`	Configure the behavior of bounces	C-, X-, and M- Series
`bvconfig`	Configure key settings for outgoing mail, and configure how to handle invalid bounces.	C- and X- Series
`certconfig`	Configure security certificates and keys	C-, X-, and M- Series
`clusterconfig`	Configure cluster related settings	C- and X- Series
`deliveryconfig`	Configure mail delivery	C- and X- Series
`destconfig`	Configure options for the Destination Controls Table.	C- and X- Series
`dictionaryconfig`	Configure content dictionaries	C-, X-, and M- Series
`dnsconfig`	Configure DNS setup	C- and X- Series
`dnslistconfig`	Configure DNS List services support	C- and X- Series
`domainkeysconfig`	Configure DomainKeys support	C- and X- Series
`encryptionconfig`	Configure email encryption	C- and X- Series

Table 1-2 CLI Commands (`commit` required) (Continued)

`etherconfig`	Configure Ethernet settings	C-, X-, and M- Series
`exceptionconfig`	Configure domain exception table	C- and X- Series
`featurekeyconfig`	Automatically check and update feature keys	C-, X-, and M-Series
`filters`	Configure message processing options	C- and X- Series
`incomingrelayconfig`	Configure Incoming Relays	C- and X- Series
`interfaceconfig`	Configure Ethernet IP addresses	C-, X-, and M- Series
`listenerconfig`	Configure mail listeners	C- and X- Series
`ldapconfig`	Configure LDAP servers	C- and X- Series
`loadconfig`	Load a configuration file	C-, X-, and M- Series
`localeconfig`	Configure multi-lingual settings	C- and X- Series
`logconfig`	Configure access to log files	C-, X-, and M- Series
`ntpconfig`	Configure NTP time server	C-, X-, and M- Series
`password or passwd`	Change your password	C-, X-, and M- Series
`policyconfig`	Configure per recipient or sender based policies	C- and X- Series
`quarantineconfig`	Configure system quarantines	C- and X- Series
`reportingconfig`	Configure reporting settings	C-, X-, and M- Series
`routeconfig`	Configure IP routing table	C-, X-, and M- Series
`scanconfig`	Configure attachment scanning policy	C- and X- Series
`senderbaseconfig`	Configure SenderBase connection settings	C- and X- Series
`setgateway`	Set the default gateway (router)	C-, X-, and M- Series

Table 1-2 CLI Commands (`commit` required) (Continued)

`sethostname`	Set the name of the machine	C-, X-, and M- Series
`settz`	Set the local time zone	C-, X-, and M- Series
`smtpauthconfig`	Configure SMTP Auto profiles	C- and X- Series
`smtproutes`	Set up permanent domain redirections	C-, X-, and M- Series
`snmpconfig`	Configure SNMP	C-, X-, and M- Series
`sshconfig`	Configure SSH keys	C-, X-, and M- Series
`stripheaders`	Set message headers to remove	C- and X- Series
`textconfig`	Configure text resources	C- and X- Series
`unsubscribe`	Update the global unsubscribe list	C-, X-, and M- Series
`updateconfig`	Configure system update parameters	C- and X- Series
`userconfig`	Manage user accounts and connections to external authentication sources.	C-, X-, and M- Series
`last`	Add, edit, and remove users	C-, X-, and M- Series
`vofconfig`	Configure Virus Outbreak Filters	C- and X- Series

CHAPTER 2

Command Line Interface: The Basics

This chapter contains the following sections:

COMMAND LINE INTERFACE (CLI)

The IronPort AsyncOS Command Line Interface is an interactive interface designed to allow you to configure and monitor the IronPort appliance. The commands are invoked by entering the command name, or in the case of batch format commands the command name with arguments (or parameters). If you enter the command without arguments, the command prompts you for the required information.

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 described in "Other Tasks in the GUI" in the *Cisco IronPort AsyncOS Daily Management Guide* to disable these services.

Accessing the Command Line Interface (CLI)

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 in the *Cisco IronPort AsyncOS Configuration Guide* 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 *Cisco IronPort AsyncOS Advanced Configuration Guide* for more information.

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

For example:

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

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

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

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

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

Command Syntax

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

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

Select Lists

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

For example:

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

Yes/No Queries

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

For example:

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

Subcommands

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

For example:

```
mail3.example.com> interfaceconfig


Currently configured interfaces:
1. Management (192.168.42.42/24: mail3.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>
```

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

Escape

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

History

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

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

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

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

Command Completion

The IronPort AsyncOS CLI 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 to IronPort AsyncOS while email operations proceed normally.

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

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

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

Note — Not all commands in AsyncOS require the `commit` command to be run. See Chapter 1, "AsyncOS 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 IronPort 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 to IronPort AsyncOS 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
Changes committed: Wed Jan 01 12:00:01 2003
```

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 changes made to the IronPort AsyncOS configuration 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 user inputs required to complete tasks and provides a mechanism allowing users to easily automate common configuration tasks. Batch commands also allow users to issue commands remotely using an SSH client. This enables users to easily script CLI commands and execute them on multiple appliances at one time.

Please note that these commands do not provide new functionality to your IronPort appliance; rather, they provide you with an additional method of execution for your appliance.

For the current release of AsyncOS these CLI commands have associated batch commands:

- `adminaccessconfig`
- `aliasconfig`
- `destconfig`
- `interfaceconfig`
- `listenerconfig -> hostacess (HAT)`
- `listenerconfig -> rcptacess (RAT)`
- `scanconfig`
- `smtproutes`
- `tlsverify`

Batch command syntax is dependent on the specific command being used. Please see the appropriate CLI example contained 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:

Table 2-1 Example `listenerconfig` command 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:
```

Table 2-1 Example `listenerconfig` command Using the CLI (Continued)

```
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> IncomingMail
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages
injected on this listener.

- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> HOSTACCESS
There are currently 4 policies defined.
There are currently 5 sender groups.

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

1. New Sender Group
2. New Policy
[1]> 1

Enter a name for this sender group. (optional)
[]> REDLIST
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are
allowed.
IP address ranges such as 10.1.1.10-20 are allowed. IP subnets such as
10.2.3. are allowed.
```

Table 2-1 Example `listenerconfig` command Using the CLI (Continued)

```
Hostnames such as crm.example.com are allowed.
Partial hostnames such as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are
allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blacklist queries such as dnslist[query.blacklist.example] are
allowed.
Separate multiple hosts with commas
[]> possible_spammer.com
Select a behavior for this entry.
1. Accept
2. Relay
3. Reject
4. TCP Refuse
5. Continue
6. Policy: ACCEPTED
7. Policy: BLOCKED
8. Policy: THROTTLED
9. Policy: TRUSTED
[1]> 8

Enter a comment for this sender group.
[]>

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

To perform the same action using a CLI batch command:

Table 2-2 Example `listenerconfig` Command Using Batch Format

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

example.com> commit
```

CHAPTER 3

The Commands: Reference Examples

This chapter contains the following sections:

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:

1. Does the command require a `commit` command to be implemented on the appliance?

2. Is the command restricted to a particular mode (cluster, group, or machine).?
3. Does the command permit a batch format?

For more information about Centralized Management, please see the *Cisco IronPort AsyncOS Advanced Configuration Guide*.

For more information about batch formats, please see "Command Line Interface: The Basics" on page 9.

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 Ironport Anti-Spam.

`Code Example 3-1` antispamconfig - IronPort Anti-Spam Configuration

```
mail3.example.com> antispamconfig

Choose the operation you want to perform:
- IRONPORT - Configure IronPort Anti-Spam.
- 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
```

Code Example 3-1 antispamconfig - IronPort Anti-Spam Configuration

```
What is the largest size message that IronPort Anti-Spam scanning
should scan?
[131072]>

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

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

IronPort Anti-Spam scanning is now enabled on the system. Please note:
you must issue the 'policyconfig' command (CLI) or Mail Policies (GUI)
to configure 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

Code Example 3-2 antispamstatus - IronPort Anti-Spam

```
mail3.example.com> antispamstatus


Choose the operation you want to perform:
- IRONPORT - Display IronPort Anti-Spam version and rule information.
- MULTISCAN - Display Intelligent Multi-Scan version and rule
information.
[]> ironport
```

Code Example 3-2 `antispamstatus` - IronPort Anti-Spam

```
  Component             Last Update                 Version
  CASE Core Files       Base Version                2.7.1-101
  Structural Rules      Base Version                2.7.1-101-
20091008_021703
  CASE Utilities        Base Version                2.7.1-101
  Web Reputation DB     Never updated               20050725_000000
  Web Reputation Rules  Never updated
20050725_000000-20050725_000000

Last download attempt made on: Never
```

antispamupdate

Description

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

Usage

This command does not require a 'commit'.

This command is restricted to machine mode.

This command does not support a batch format.

Example

Code Example 3-3 `antispamupdate`

```
mail3.example.com> antispamupdate

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 RelaysConfiguring an Incoming Relay

Code Example 3-4 incomingrelayconfig

```
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 IronPort appliance determine the sender's
originating IP address.

You should ONLY enable this command if your 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 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. 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.
```

Code Example 3-4 incomingrelayconfig

```
[]> 192.168.1.1

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

Within the "Received:" header, enter the special character or string
after which to begin parsing for the originating IP address:
[from]> [

Within the headers, enter the position of the "Received:" header that
contains the originating IP address:

[1]> 1

There is 1 relay defined.

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

Incoming                        Header            Match       Received
relay name:    IP address:      to parse:         after:      position:
-----------    -----------      ---------         ------      ---------
first-hop      192.168.1.1      Received          [           1

There is 1 relay defined.

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

Enter a name for this incoming relay (Ex: "first-hop")
[]> second-hop

Enter the IP address of the incoming relay. CIDR addresses such as
```

Code Example 3-4 incomingrelayconfig

```
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.
[]> 192.168.1.2

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

1. Use "Received:" header
2. Use a custom header
[1]> 2

Enter the custom header name that contains the originating IP address:
[]> X-Connecting-IP

There are 2 relays defined.

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

Incoming                        Header            Match       Received
relay name:    IP address:      to parse:         after:      position:
-----------    -----------      ---------         ------      ---------
first-hop      192.168.1.1      Received          [           1
second-hop     192.168.1.2      X-Connecting-IP   n/a         n/a

There are 2 relays defined.

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

1. first-hop:      192.168.1.1
2. second_hop:     192.168.1.2
Enter the number of the entry you wish to delete:
[1]> 1
```

Code Example 3-4 incomingrelayconfig

```
Incoming relay "first-hop" deleted.

There is 1 relay defined.
```

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 95.

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

Code Example 3-5 `antivirusconfig`

```
mail3.example.com> antivirusconfig

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
```

Code Example 3-5 `antivirusconfig` (Continued)

```
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.
[]>

mail3.example.com>
```

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:

Code Example 3-6 `antivirusconfig` - Viewing IDE Details

```
mail3.example.com> antivirusconfig

Sophos Anti-Virus: Enabled

Choose the operation you want to perform:
- SETUP - Configure Sophos Anti-Virus.
- STATUS - View Sophos Anti-Virus status.
- DETAIL - View Sophos Anti-Virus detail.
[]> detail

Sophos Anti-Virus:

Product - 3.87
Engine - 2.25.0
Product Date - 01 Nov 2004


Sophos IDEs currently on the system:

   'Mkar-E.Ide'          Virus Sig. - 23 Dec 2004 01:24:02
   'Rbot-Sd.Ide'         Virus Sig. - 22 Dec 2004 19:10:06
   'Santy-A.Ide'         Virus Sig. - 22 Dec 2004 06:16:32
   'Bacbanan.Ide'        Virus Sig. - 21 Dec 2004 18:33:58
```

Code Example 3-6 `antivirusconfig` - Viewing IDE Details (Continued)

```
   'Rbot-Sb.Ide'          Virus Sig. - 21 Dec 2004 14:50:46
   'Rbotry.Ide'           Virus Sig. - 21 Dec 2004 06:13:40
   'Sdbot-Si.Ide'         Virus Sig. - 20 Dec 2004 20:52:04
   'Oddbob-A.Ide'         Virus Sig. - 19 Dec 2004 23:34:06
   'Rbot-Rw.Ide'          Virus Sig. - 19 Dec 2004 00:50:34
   'Wortd.Ide'            Virus Sig. - 18 Dec 2004 07:02:44
   'Delf-Jb.Ide'          Virus Sig. - 17 Dec 2004 22:32:08
[...command continues...]
```

antivirusstatus

Description

Display Anti-Virus status.

Usage

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

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

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

Example

Code Example 3-7 `antivirusstatus`

```
mail3.example.com> antivirusstatus

   SAV Engine Version        3.85
   IDE Serial                2004101801
 Engine Update        Mon Sep 27 14:21:25 2004
   Last IDE Update           Mon Oct 18 02:56:48 2004
   Last Update Attempt       Mon Oct 18 11:11:44 2004
   Last Update Success       Mon Oct 18 02:56:47 2004

mail3.example.com>
```

antivirusupdate

Description

Manually update virus definitions.

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

Code Example 3-8 `antivirusupdate`

```
mail3.example.com> antivirusupdate

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 ?
- 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.

Code Example 3-9 `commit`

```
mail3.example.com> commit

Please enter some comments describing your changes:

[]> Changed "psinet" IP Interface to a different IP ad dress
Changes committed: Wed Apr 13 12:00:01 2005
```

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

Code Example 3-10 commitdetail

```
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 changes made to the IronPort AsyncOS configuration 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

Code Example 3-11 `clear`

```
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

Code Example 3-12 `help`

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

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

Code Example 3-13 `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
```

CONFIGURATION FILE MANAGEMENT

This section contains the following CLI commands:

- loadconfig
- mailconfig
- resetconfig
- saveconfig
- showconfig

loadconfig

Description

Load a configuration file.

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.

Code Example 3-14 `loadconfig` -

```
mail3.example.com> loadconfig

1. Paste via CLI
2. Load from file
[1]> 2

Enter the name of the file to import:
[]> 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:
[]> loaded new configuration file
```

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.

Code Example 3-15 `loadconfig` - Example 2

```
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
```

mailconfig

Description

To test the IronPort AsyncOS 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

Code Example 3-16 `mailconfig`

```
mail3.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

The configuration file has been sent to user@example.com.
mail3.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* IronPort AsyncOS 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

Code Example 3-17 `resetconfig`

```
mail3.example.com> offline

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.

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

Code Example 3-18 `saveconfig`

```
mail3.example.com> saveconfig

Do you want to include passwords? Please be aware that a configuration
without passwords will fail when reloaded with loadconfig.  [N]> y

The file C60-00065B8FCEAB-31PM121-20030630T130433.xml has been saved
in the configuration directory.
mail3.example.com>
```

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

Code Example 3-19 `showconfig`

```
ail3.example.com> showconfig

Do you want to include passwords? Please be aware that a configuration
without passwords will fail when reloaded with loadconfig.

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">

<!--
  Product: IronPort model number Messaging Gateway Appliance(tm)
  Model Number: model number
  Version: version of AsyncOS installed
  Serial Number: serial number
  Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

CLUSTER MANAGEMENT

This section contains the following CLI commands:

- clusterconfig
- clustercheck

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 supports a batch format.

Example

For an explanation of the `clusterconfig` command and its uses, please see the *IronPort AsyncOS 4.6 Advanced User Guide*.

clustercheck

Description

The `clustercheck` command checks that all configuration databases in the cluster are sychronized.

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

For an explanation of the `clustercheck` command and its uses, please see the *Cisco IronPort AsyncOS Advanced Configuration Guide*.

DOMAIN KEYS

This section contains the following CLI commands:

- domainkeysconfig

domainkeysconfig

Description

Configure DomainKeys support.

Note — This command is restricted on C670 Email Security appliances with a FIPS-compliant Hardware Security Module card. Only the to only the `publickey`, `list`, and `print` options are available for the `keys` subcommand.Use the `fipsconfig` -> `domainkeysconfig` command instead. For more information, see "fipsconfig" on page 78.

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: Configuring Domain Keys via the CLI

Use the `domainkeysconfig` command in the CLI to configure Domain Keys on your IronPort 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" on page 46.

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

Code Example 3-20 `domainkeysconfig` - Example 1

```
mail3.example.com> domainkeysconfig

Number of Domain Profiles: 0
Number of Signing Keys: 0

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SEARCH - Search for domain profile or key.
[]> keys

No signing keys are defined.
```

Code Example 3-20 `domainkeysconfig` - Example 1 (Continued)

```
Choose the operation you want to perform:
- NEW - Create a new signing key.
- IMPORT - Import signing keys from a file.
[]> new

Enter a name for this signing key:
[]> TestKey

1. Generate a private key
2. Enter an existing key
[1]>
1. 512
2. 768
3. 1024
4. 1536
5. 2048
[3]>
New key "TestKey" created.

There are currently 1 signing keys defined.

Choose the operation you want to perform:
- NEW - Create a new signing key.
- EDIT - Modify a signing key.
- PUBLICKEY - Create a publickey from a signing key.
- DELETE - Delete a signing key.
- PRINT - Display signing keys.
- IMPORT - Import signing keys from a file.
- EXPORT - Export signing keys to a file.
- CLEAR - Clear all signing keys.
[]>

Number of Domain Profiles: 0
Number of Signing Keys: 1

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SEARCH - Search for domain profile or key.
[]> profiles


No domain profiles are defined.

Choose the operation you want to perform:
```

Code Example 3-20 `domainkeysconfig` - Example 1 (Continued)

```
- NEW - Create a new domain profile.
- IMPORT - Import domain profiles from a file.
[]> new

Enter a name for this domain profile:
[]> Example

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 values
becomes the "d" tag of the Domain-Keys signature.
Enter the domain name of the signing domain:
[]> example.com

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


Enter selector:
[]> test

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 "nofws".
Select canonicalization algorithm:
1. simple
2. nofws
[2]>

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 Domain Keys 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
```

Code Example 3-20 `domainkeysconfig` - Example 1 (Continued)

```
[1]>

Finish by entering profile users.  The following types of entries are
allowed:
- Email address entries such as "joe@examples.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.examples.com".
 This sort of entry will not match the root domain ("example.com").

Enter user for this signing profile:
[]> sales.example.com

Do you want to add another user? [N]>

There are currently 1 domain profiles defined.

Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- 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.
[]>
mail3.example.com> commit
```

Creating a Sample Domain Keys DNS TXT Record

Code Example 3-21 `domainkeysconfig` - Example 2

```
mail3.example.com> domainkeysconfig

Number of Domain Profiles: 1
Number of Signing Keys: 1

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SEARCH - Search for domain profile or key.
[]> profiles

There are currently 1 domain profiles defined.
Choose the operation you want to perform:
```

Code Example 3-21 `domainkeysconfig` - Example 2

```
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]> dnstxt

Enter the name or number of a domain profile.
1. Example
[1]>

The answers to the following questions are used to construct the tags
of a sample DomainKeys DNS TXT record.  This record can be used to
publish this domain profile's public DomainKeys information in the
DNS.

Do you wish to constrain the local part of the sending address
associated with this domain profile? (This is the "g" tag of
DomainKeys DNS TXT record.)


Constrain local part of sending address? [N]>

The "k" tag is used to specify the key type of the publish key.  At
this time the only supported key type is 'rsa'. This tag is optional,
and can be included to improve the readability of the DNS TXT record.

Include the "k" tag? [N]>

Notes that may be of interest to a human can be included in the TXT
record under the "n" tag.  No interpretation is made by any program.

Include the "n" tag? [N]>

The "testing mode" tag can be set to specify that this domain is
testing DomainKeys and that unverified email must not be treated
differently from verified email.

Include the "t" (testing mode) tag? [N]>
The DomainKeys DNS TXT record is:
```

Code Example 3-21 `domainkeysconfig` - Example 2

```
test._domainkey.example.com IN TXT
"p=rh0DF7SH+Yvywe0FaxnOEoxzzZyFCf3KEAy4oE+x9Wm40g9JrMhFiboZ9TgoDTPdXQ
NgOLDiH9ngxarJN9y9XBglVJTYMuq4SEI97WjMUeGC0XQ10q3zHYpd+usPFmwwIDAQAB;
"

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.
- 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.
[]>

Number of Domain Profiles: 1
Number of Signing Keys: 1

Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SEARCH - Search for domain profile or key.
[]>

mail3.example.com> commit
```

DNS

This section contains the following CLI commands:

- dnsconfig
- dnsflush
- dnslistconfig
- dnslistflush
- dnslisttest
- dnsstatus

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 does not support a batch format.

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 3-1 Subcommands for `dnsconfig` Command

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

Code Example 3-22 `dnsconfig`

```
mail3.example.com> dnsconfig

Currently using the local DNS cache servers:
1. dns.example.com (10.1.10.9)

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]> setup

Do you want the Gateway to use the Internet's root DNS servers or
would you like it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use own DNS cache servers
[1]> 1

Choose the IP interface for DNS traffic.
1. Auto
2. Management (100.100.10.15/24)
[1]> 1

Enter the number of seconds to wait before timing out reverse DNS
lookups.
[20]>

Currently using the Internet root DNS servers.

No alternate authoritative servers configured.

Enter the number of seconds to wait before timing out reverse DNS
lookups.
[20]>

Choose the operation you want to perform:
- NEW - Add a new server.
- SETUP - Configure general settings.
[]>

mail3.example.com>
```

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.

Code Example 3-23 `dnsconfig` -Adding Alternate DNS Servers

```
mail3.example.com> dnsconfig

Currently using the Internet root DNS servers.

No alternate authoritative servers configured.

Enter "NEW" to add a server, "DELETE" to remove, "EDIT" to modify,
or "SETUP" for general settings.
[]> new

Please enter the domain this server is authoritative for. (Ex: "com").
[]> example.com

Please enter the fully qualified hostname of the DNS server for
the domain "example.com".
(Ex: "dns.example.com").
[]> dns.example.com

Please enter the IP of dns.example.com.
[]> 10.1.10.9

Enter the number of seconds to wait before timing out reverse DNS
lookups.
[20]>

Currently using the Internet root DNS servers.

Alternate authoritative DNS servers:
1. example.com: dns.example.com (10.10.200.1)

Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
mail3.example.com>
```

Using Your Own DNS Cache Servers

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

Code Example 3-24 `dnsconfig` - Using your own DNS cache servers

```
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.
- 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.
[]> dnsmain.example.com

The IP address must be 4 numbers separated by a period.  Each number
must be a value from 0 to 255. (Ex: 192.168.1.1)
Please enter the IP address of your DNS server.
Separate multiple IPs with commas.
[]> 10.10.200.03

Please enter the priority for 10.10.200.3.
A value of 0 has the highest priority.
The IP will be chosen at random if they have the same priority
[1]> 1

Choose the IP interface for DNS traffic.
1. Auto
2. Management (192.168.42.42/24)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1

Enter the number of seconds to wait before timing out reverse DNS
lookups.
```

Code Example 3-24 `dnsconfig` - Using your own DNS cache servers (Continued)

```
[20]>
Currently using the local DNS cache servers:

1. dnsmain.example.com (10.10.200.03)

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

Code Example 3-25 `dnsflush`

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

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

Code Example 3-26 `dnslistconfig`

```
mail3.example.com> dnslistconfig

Current DNS List Settings:
Negative Response TTL:  1800 seconds
DNS List Query Timeout:  3 seconds

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

Enter the cache TTL for negative responses in seconds:
[1800]> 1200

Enter the query timeout in seconds:
[3]>

Settings updated.

Current DNS List Settings:
Negative Response TTL:  1200 seconds
DNS List Query Timeout:  3 seconds

Choose the operation you want to perform:
- SETUP - Configure general settings.
[]>

mail3.example.com>
```

dnslistflush

Description

Flush the current DNS List 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

Code Example 3-27 `dnslistflush`

```
mail3.example.com> dnslistflush

Are you sure you want to clear out the DNS List cache? [N]> y

DNS List cache has been cleared.
mail3.example.com>
```

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

Code Example 3-28 `dnslisttest`

```
mail3.example.com> dnslisttest

Enter the query server name:
[]> mail4.example.com

Enter the test IP address to query for:
[127.0.0.2]> 10.10.1.11

Querying:  10.10.1.11.mail4.example.com
Result:  MATCHED
mail3.example.com>
```

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

Code Example 3-29 `dnsstatus`

```
mail3.example.com> dnsstatus

Status as of: Mon Apr 18 10:58:07 2005 PDT

Counters:                    Reset          Uptime        Lifetime
  DNS Requests               1,115           1,115           1,115
  Network Requests             186             186             186
  Cache Hits                 1,300           1,300           1,300
  Cache Misses                   1               1               1
  Cache Exceptions               0               0               0
  Cache Expired                185             185             185

mail3.example.com>
```

GENERAL MANAGEMENT/ADMINISTRATION/TROUBLESHOOTING

This section contains the following CLI commands:

- addressconfig
- adminaccessconfig
- certconfig
- diagnostic
- encryption
- featurekey
- featurekeyconfig
- fipsconfig
- ntpconfig
- reboot
- resume
- resumedel
- resumelistener
- settimesettz
- shutdown
- sshconfig
- status
- supportrequest
- suspend
- suspenddel
- suspendlistener
- techsupport
- tlsverify
- trace
- updateconfig
- version
- upgrade

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 circumstatnces:

- Anti-virus notifications
- Bounces
- Notifications (`notify()` and `notify-copy()` filter actions)
- tine notifications (`duplicate()` filter action)

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.

Code Example 3-30 `addressconfig`

```
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>

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.
- 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
```

Code Example 3-30 `addressconfig` (Continued)

```
Do you want the virtual gateway domain used for the domain? [Y]> n

Please enter the domain name portion of the "notify from" address
[None]> 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>

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.
[]>
```

adminaccessconfig

Description

Configure network access list and banner login.

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 fuctions 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>
```

- 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
```

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 three sets of IP addresses:

Code Example 3-31 adminaccessconfig - Network Access List

```
mail3.example.com> adminaccessconfig


Choose the operation you want to perform:
- BANNER - Configure login message(banner) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative
interface.
[]> ipaccess

Current mode: Allow All.
```

Code Example 3-31 adminaccessconfig - Network Access List

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

Code Example 3-31 adminaccessconfig - Network Access List

```
Please enter IP address, subnet or range.
[]> 192.168.2.2


List of allowed IP addresses/Subnets/Ranges:

1.  192.168.1.2-100
2.  192.168.255.12
3.  192.168.2.2

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 [192.168.8.126] 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]> n

List of allowed IP addresses/Subnets/Ranges:

1.  192.168.1.2-100
2.  192.168.255.12
3.  192.168.2.2

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.
[]> 192.168.8.126


List of allowed IP addresses/Subnets/Ranges:

1.  192.168.1.2-100
2.  192.168.255.12
3.  192.168.2.2
4.  192.168.8.126
```

Code Example 3-31 adminaccessconfig - Network Access List

```
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.
[]>

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.
[]>
```

Example - Configuring Network Access List

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:

Code Example 3-32 adminaccessconfig - Banner List

```
Choose the operation you want to perform:
- BANNER - Configure login message(banner) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
[]> 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.
```

Code Example 3-32 adminaccessconfig - Banner List

```
^D

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.
[]>
```

certconfig

Description

Configure security certificates and keys.

Note — This command is restricted on C670 Email Security appliances with a FIPS-compliant Hardware Security Module card. Only the to only the `print` option is available for the `certitificate` subcommand. Use the `fipsconfig` -> `certconfig` command instead. For more information, see "fipsconfig" on page 78.

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.

Code Example 3-33 `certconfig` - Pasting in a certificate

```
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
[]> certificate

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  -------
--
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3467 days
```

Code Example 3-33 `certconfig` - Pasting in a certificate

```
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-----
MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgaAxCzAJBgNVBAYTAlBUMRMwEQYD
VQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5ldXJv
bmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZpMB4X
DTk2MDkwNTAzNDI0M1oXDTk2MTAwNTAzNDI0M1owgaAxCzAJBgNVBAYTAlBUMRMw
EQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5l
dXJvbmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMT
EmJydXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNw
L4lYKbpzzlmC5beaQXeQ2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAATAN
BgkqhkiG9w0BAQQFAANBAFqPEKFjk6T6CKTHvaQeEAsX0/8YHPHqH/9AnhSjrwuX
9EBc0n6bVGhN7XaXd6sJ7dym9sbsWxb+pJdurnkxjx4=
-----END CERTIFICATE-----
.
C=PT,ST=Queensland,L=Lisboa,O=Neuronio,
Lda.,OU=Desenvolvimento,CN=brutus.partner.com,emailAddress=admin@example.com

Paste private key in PEM format (end with '.'):
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNwL4lYKbpzzlmC5beaQXeQ
2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAAQJBALjkK+jc2+iihI98riEF
oudmkNziSRTYjnwjx8mCoAjPWviB3c742eO3FG4/soi1jD9A5alihEOXfUzloenr
8IECIQD3B5+0l+68BA/6d76iUNqAAV8djGTzvxnCxycnxPQydQIhAMXt4trUI3nc
a+U8YL2HPFA3gmhBsSICbq2OptOCnM7hAiEA6Xi3JIQECob8YwkRj29DU3/4WYD7
WLPgsQpwo1GuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IZmxdcLpRcpslpeWBBAiEA
6/5B8J0GHdJq89FHwEG/H2eVVUYu5y/aD6sgcm+0Avg=
-----END RSA PRIVATE KEY-----
.

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


List of Certificates
```

Code Example 3-33 `certconfig` - Pasting in a certificate

```
Name       Common Name           Issued By             Status         Remaining
--------  -------------------  --------------------  -------------  ---------
partner.c brutus.partner.com   brutus.partner       Active        30 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active        3467 days

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


Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
[]>

esx16-esa01.qa> commit
Please enter some comments describing your changes:
[]> Installed certificate and key for receiving, delivery, and https
```

Example - Creating a self-signed certificate

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

Code Example 3-34 `certconfig` - Creating a self-signed certificate

```
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
[]> 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
```

Code Example 3-34 `certconfig` - Creating a self-signed certificate

```
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

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 Francisoc

Enter State or Province:
> CA

Enter Country (2 letter code):
> US

Duration before expiration (in days):
[3650]>

1. 1024
2. 2048
Enter size of private key:
[2]>

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

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDELMAkGA1UEBhMCVVMxFDASBgNVBAMTC2V4YW1wbGUuY29t
MRYwFAYDVQQHEw1TYW4gRnJhbmNpc29jMRAwDgYDVQQKEwdleGFtcGxlMQswCQYD
```

Code Example 3-34 `certconfig` - Creating a self-signed certificate

```
VQQIEwJDQTEMMAoGA1UECxMDb3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA+NwamZyX7VgTZka/x1I5HHrN9V2MPKXoLq7FjzUtiIDwznElrKIuJovw
Svonle6GvFlUHfjv8B3WobOzk5Ny6btKjwPrBfaY+qr7rzM4lAQKHM+P6l+lZnPU
P05N9RCkLP4XsUuyY6Ca1WLTiPIgaq2fR8Y0JX/kesZcGOqlde66pN+xJIHHYadD
oopOgqi6SLNfAzJu/HEu/fnSujG4nhF0ZGlOpVUx4fg33NwZ4wVl0XBk3GrOjbbA
ih9ozAwfNzxb57amtxEJk+pW+co3uEHLJIOPdih9SHzn/UVU4hiu8rSQR19sDApp
kfdWcfaDLF9tnQJPWSYoCh0USgCc8QIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEB
AGiVhyMAZuHSv9yA08kJCmrgO89yRlnDUXDDo6IrODVKx4hHTiOanOPu1nsThSvH
7xV4xR35T/QV0U3yPrL6bJbbwMySOLIRTjsUcwZNjOE1xMM5EkBM2BOI5rs4l59g
FhHVejhG1LyyUDL0U82wsSLMqLFH1IT63tzwVmRiIXmAu/lHYci3+vctb+sopnN1
lY1OIuj+EgqWNrRBNnKXLTdXkzhELOd8vZEqSAfBWyjZ2mECzC7SG3evqkw/OGLk
AilNXHayiGjeY+UfWzF/HBSekSJtQu6hIv6JpBSY/MnYU4tllExqD+GX3lru4xc4
zDas2rS/Pbpn73Lf503nmsw=
-----END CERTIFICATE REQUEST-----

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  ------------------- --------------------  -------------  ---------
example.c  example.com           example.com           Valid          3649 days
partner.c  brutus.partner.com    brutus.partner.com   Valid          30 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3467 days

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

diagnostic

Description

The diagnostic command is used to check RAID disks, view and clear cache information, and to test connectivity to other mail servers.

Using the `diagnostic` Command

The following commands are available within the `diagnostic` submenu:

Table 3-2 `diagnostic` Subcommands

Option	Sub commands	Availability
`RAID`	1. Run disk verify	Available on C30 and C60 only.
	2. Monitor tasks in progress	
	3. Display disk verify verdict	
`NETWORK`	FLUSH	C-, X-, and M-Series
	ARPSHOW	
	SMTPPING	
	TCPDUMP	

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:

- Check the RAID status

```
diagnostic raid
```

- Clear the LDAP, DNS and ARP caches

```
diagnostic network flush
```

- Display the ARP cache:

```
diagnostic network arpshow
```

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.

Code Example 3-35 diagnostic

```
mail3.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
[]> arpshow

System ARP cache contents:

(163.17.0.1) at 00:02:b1:cf:10:11 on fxp0 [ethernet]

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
[]> flush

Flushing LDAP cache.
Flushing DNS cache.
Flushing DNS List cache.
Flushing system ARP cache.
163.17.0.1 (163.17.0.1) 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.

Code Example 3-36 diagnostic: SMTPPING

```
mail3.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
```

Code Example 3-36 diagnostic: SMTPPING

```
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.

[]> smtpping
Enter the hostname or IP address of the SMTP server:
[mail3.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. d1.mail.com
2. d2.mail.com
3. mail.com
[1]> 3

Select a network interface to use for the test.
1. Data 1
2. Data 2
3. Management
4. auto
[4]> 3

Using interface 'Management' with source IP 168.18.0.220.
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]>n

Starting SMTP test of host mail.com.
Resolved 'mail.com' to 166.11.0.6.
Connection to 166.11.0.6 succeeded.
Command EHLO succeeded
Command MAIL FROM succeeded.
Test complete. Total time elapsed 0.01 seconds
```

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:

Code Example 3-37 encryptionconfig

```
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]> y


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
```

Code Example 3-37 encryptionconfig

```
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Return receipts enabled: Yes
Envelope sensitivity: High
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Text notification template: System Generated
HTML notification template: System Generated
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- RECEIPT - Change return receipt handling
- SENSITIVITY - Change envelope sensitivity
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- 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
[]> sensitivity

1. Medium (password required to open envelopes, but credentials may be
cached)
2. High (password required and passphrase enabled, and credentials may
not be cached)
3. No Password Required (The recipient does not need a password to
open the encrypted message.)
Please enter the envelope sensitivity level:
[2]> 1

Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Return receipts enabled: Yes
Envelope sensitivity: High
Secure Forward enabled: No
```

Code Example 3-37 encryptionconfig

```
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Text notification template: System Generated
HTML notification template: System Generated
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- RECEIPT - Change return receipt handling
- SENSITIVITY - Change envelope sensitivity
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- 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
[]> forward

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

Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Return receipts enabled: Yes
Envelope sensitivity: High
Secure Forward enabled: Yes
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Text notification template: System Generated
HTML notification template: System Generated
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated

Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- RECEIPT - Change return receipt handling
```

Code Example 3-37 encryptionconfig

```
- SENSITIVITY - Change envelope sensitivity
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- 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
[]>

Proxy: Not Configured

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

encryptionstatus

Description

The `encryptionstatus` command shows the version of the PXE Engine and Domain Mappings file on the IronPort 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

Code Example 3-38 encryptionstatus

```
mail3.example.com> encryptionstatus

Component                 Version    Last Updated
PXE Engine                6.7.1      17 Nov 2009 00:09 (GMT)
Domain Mappings File      1.0.0      Never updated
```

encryptionupdate

Description

The `encryptionupdate` command requests an update to the PXE Engine on the IronPort Email Security 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

Code Example 3-39 encryptionupdate

```
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.

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.

Code Example 3-40

```
mail3.example.com> featurekey
Module                        Quantity   Remaining   Expiration Date
Bounce Verification           1          30 days     Fri Jun 30 18:57:26 2006
IronPort Anti-Spam            1          28 days     Thu Jun 29 15:20:23 2006
Incoming Mail Handling        1          28 days     Thu Jun 29 15:20:31 2006
Virus Outbreak Filters        1          28 days     Thu Jun 29 15:20:24 2006
Sophos Anti-Virus             1          28 days     Thu Jun 29 15:20:23 2006
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.

Code Example 3-41 featurekeyconfig

```
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
```

fipsconfig

Description

The `fipsconfig` command configures the Hardware Security Module (HSM) card and the Federal Information Processing Standard (FIPS) settings for C670 Email Security appliances with an HSM card. When you enter `fipsconfig` at the command line, the CLI prompts you to enter the FIPS Officer password. The default password is `sopin123`.

The fipsconfig command allows you to perform the following:

- `init` - Initializes the HSM card and reboots the appliance.
- `getinfo` - Displays the HSM card status.
- `certconfig` - Configures the certificates and keys for services on the Email Security appliance. This is similar to the `certconfig` command. See "certconfig" on page 64 for more information.
- `domainkeysconfig` - Configures keys for DKIM and DomainKeys signing. This is similar to the domainkeysconfig command. See "domainkeysconfig" on page 43 for more information.
- `clonetarget` - Clones the HSM card as a target when copying the master key among multiple HSM cards.
- `clonesource` - Clones the HSM card as a source when copying the master key among multiple HSM cards.
- `passwd` - Changes the FIPS password.
- `backup` and `restore` - Backs up and restores critical security parameters.

Note — This command is not available on appliances that do not have an HSM card. Only administrators with the FIPS officer password can use the command. The HSM card will be reset if you enter the incorrect FIPS Officer password three times.

Usage

Commit: This command does not require 'commit'.

Cluster Management: This command is available only at the machine level.

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

Example

The following example shows how to display the HSM card status.

`Code Example 3-42 fipsconfig`

```
c670q03.qa> fipsconfig

WARNING: Entering wrong password for Crypto Officer three times will
erase all critical information on the HSM card.
Enter the Crypto Officer password:
```

Code Example 3-42 fipsconfig

```
Choose the operation you want to perform:
- INIT - Initialize the hardware security module.
- GETINFO - Display the hardware security module status.
- CERTCONFIG - Configure certificates and keys.
- DOMAINKEYSCONFIG - Configure keys for DomainKeys and DKIM.
- CLONETARGET - Clone the hardware security module as the target.
- CLONESOURCE - Clone the hardware security module as the source.
- BACKUP - Backup critical security parameters.
- RESTORE - Restore critical security parameters.
- PASSWD - Change FIPS password.
[]> getinfo

Firmware Version: 4.7.1
Serial Number: 8100752
Hardware ID: K5
Label: Cisco_IronPort_Label

Total SRAM Memory: 16984932
Free SRAM Memory: 16983492
Total Flash Memory: 14286412
Free Flash Memory: 14281236

FIPS capabilities and policy values:
                                    Capability    Policy
Enable PIN Authentication           1             1
Enable PED Authentication           1             0
Performance Level                   4             -
M of N Code                         0             0
Enable Configuration Masking        1             1
Allow Configuration Cloning         1             1
Allow Non-FIPS Algorithms           1             0
Allow Network Replication           0             0
Allow Offboard Storage              1             1
Private Key Wrapping                0             0
Secret Key Wrapping                 1             1
Allow Changing Key Attributes       1             1
Authentication Without Challenge    1             1
Allow Non-Local Signing Key         1             1
Maximum Failed Login Attempts       10            10
Allow Auto-Activation               1             0

Choose the operation you want to perform:
- INIT - Initialize the hardware security module.
- GETINFO - Display the hardware security module status.
```

Code Example 3-42 fipsconfig

```
- CERTCONFIG - Configure certificates and keys.
- DOMAINKEYSCONFIG - Configure keys for DomainKeys and DKIM.
- CLONETARGET - Clone the hardware security module as the target.
- CLONESOURCE - Clone the hardware security module as the source.
- BACKUP - Backup critical security parameters.
- RESTORE - Restore critical security parameters.
- PASSWD - Change FIPS password.
[]>
```

ntpconfig

Description

The `ntpconfig` command configures IronPort 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

Code Example 3-43 `ntpconfig`

```
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
```

Code Example 3-43 `ntpconfig` (Continued)

```
2. bitsy.mit.edi

Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries
should
originate.
[]> sourceint

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

Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries
should originate.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added new NTP server

Changes committed: Thu Mar 27 15:01:27 2003
```

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

Code Example 3-44 `reboot`

```
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.
```

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

Code Example 3-45 `resume`

```
mail3.example.com> resume

Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

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

Code Example 3-46 `resumedel`

```
mail3.example.com> resumedel

Mail delivery resumed.
```

resumelistener

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

Code Example 3-47 `resumelistener`

```
mail3.example.com> resumelistener

Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1

Receiving resumed.
mail3.example.com>
```

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

Code Example 3-48 `settime`

```
mail3.example.com> settime

WARNING: Changes to system time will take place immediately
and do not require the user to run the commit command.
Current time 09/23/2001 21:03:53.
This machine is currently running NTP.
In order to manually set the time, NTP must be disabled.
Do you want to stop NTP and manually set the time? [N]> Y

Please enter the time in MM/DD/YYYY HH:MM:SS format.
[]> 09/23/2001 21:03:53

Time set to 09/23/2001 21:03:53.
```

settz

Description

Set the local time zone.

Usage

Commit: This command requires a 'commit'.

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

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

Example

Code Example 3-49 `settz`

```
mail3.example.com> settz

Current time zone: America/Los_Angeles

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
```

Code Example 3-49 `settz` (Continued)

```
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.
[]>

mail3.example.com>
```

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

Code Example 3-50 shutdown

```
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 keys.

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.

Example

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

Code Example 3-51 sshconfig - Install a New Public Key for the 'Admin' Account

```
mail3.example.com> sshconfig

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.
- SETUP -  Configure general settings.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.

[cut and paste public key for user authentication here]

Currently installed keys for admin:
1. ssh-dss AAAAB3NzaC1kc3MAA...CapRrgxcY= (admin@example.com)
```

Code Example 3-51 sshconfig - Install a New Public Key for the 'Admin' Account (Continued)

```
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- PRINT - Display a key.
[]>
```

Disabling SSH1

To disable (or enable) SSH1, use the `setup` subcommand of the `sshconfig` command:

Code Example 3-52 `sshconfig` - Enabling/Disabling SSH1

```
mail3.example.com> sshconfig

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.
- SETUP -  Configure general settings.
[]> setup

Choose the operation you want to perform:
- DISABLE - Disable SSH v1
[]> disable

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.
- SETUP - Configure general settings
[]>

mail3.example.com> commit
```

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

Code Example 3-53 `status`

```
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

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

Gauges:                                  Current
  Connections
    Current Inbound Conn.                      0
    Current Outbound Conn.                    14
  Queue
    Active Recipients                      7,166
    Messages In Work Queue                     0
    Messages In Quarantine                16,248
    Kilobytes Used                       387,143
      Kilobytes In Quarantine            338,206
    Kilobytes Free                    39,458,745


mail3.example.com>
```

supportrequest

Description

Send a message to IronPort Customer Care. 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.

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.

Code Example 3-54 supportrequest

```
mail3.example.com> supportrequest

Do you want to send the support request to
supportrequest@ironport.com? [Y]> y

Do you want to send the support request to additional recipient(s)?
[N]> y

Please enter the email address(es) to which you want to send the
support request.  Include anyone in your organization that should be
included on future correspondence for this issue.  Separate multiple
addresses with commas.
[]> administrator@example.com, postmaster@example.com

Is this support request associated with an existing support ticket?
[N]> n

Please enter some comments describing your issue, providing as much
detail as possible to aid in diagnosing any issues:

[]> Having DNS resolution issues with some domains

For future correspondence on this issue, please enter your email
address:
[]> mail3@example.com
```

Code Example 3-54 supportrequest

```
Please enter any additional contact information (e.g. phone
number(s)):
[]> (650)555-1212 (office), (650)555-1212 (cell)

Generating configuration information; this will take about 10
seconds...

The support request information has been sent to
supportrequest@ironport.com, administrator@example.com,
postmaster@example.com.

Do you want to print the support request to the screen? [N]> n
```

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

Code Example 3-55 suspend

```
mail3.example.com> suspend

Enter the number of seconds to wait before abruptly closing
connections.
[30]> 45

Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com>
```

suspenddel

Description

Suspend deliveries

Usage

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

Cluster Management: This command is restricted to machine mode.

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

Example

Code Example 3-56 `suspenddel`

```
mail3.example.com> suspenddel

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

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

Code Example 3-57 `suspendlistener`

```
mail3.example.com> suspendlistener

Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1

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

Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

techsupport

Description

Allow IronPort customer service 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

Code Example 3-58 `techsupport`

```
mail3.example.com> techsupport

S/N XXXXXXXXXXX-XXXXXXX
Service Access currently disabled.

Choose the operation you want to perform:
- ENABLE - Allow an IronPort customer service representative to
remotely access your system to assist you in solving your technical
issues.
- STATUS - Display the current techsupport status.
[]> enable

Enter a temporary password for customer care to use.  This password may
not be the same as your admin password.  This password will not be able
to be used to directly access your system.
[]> **********

Are you sure you want to enable service access? [N]> y

Service access has been ENABLED.  Please provide your temporary
password to your IronPort Customer Care representative.
S/N 00065BF3BA6D-9WFWC21
Service Access currently ENABLED (0 current service logins).

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

tlsverify

Description

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

Usage

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

Cluster Management: This command is restricted to machine mode.

Batch Command: This command supports a batch format.

Batch Format

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

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

Example

Code Example 3-59 tlsverify

```
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

Code Example 3-60 `trace`

```
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)
```

Code Example 3-60 `trace` (Continued)

```
 - 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'

VOF Evaluation:
 - No threat detected
```

Code Example 3-60 `trace` (Continued)

```
Message Enqueued for Delivery

Would you like to see the resulting message? [Y]> y


Final text for messages matched on policy Management Upgrade
Final Envelope Sender:  pretend.sender@example.doma
Final Recipients:
 - admin@ironport.com

Final Message Content:

Received: from remotehost.example.com (HELO TEST) (1.2.3.4)
  by stacy.qa with TEST; 19 Oct 2004 00:54:48 -0700
Message-Id: <3i93q9$@Management>
X-IronPort-AV: i="3.86,81,1096873200";
   d="scan'208"; a="0:sNHT0"
Subject: hello

This is a test message.

Run through another debug session? [N]>
```

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

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.

Example

In the following example, the updateconfig commad is used to configure the appliance to download update images from IronPort servers and download the list of available AsyncOS upgrades from a local server.

Code Example 3-61 updateconfig

```
mail3.example.com> updateconfig

Service (images):                 Update URL:

-------------------------------------------------------------------------------
Sophos Anti-Virus definitions     http://downloads.ironport.com/av
IronPort Anti-Spam rules          http://downloads.ironport.com/as
Intelligent Multi-Scan rules      http://downloads.ironport.com/as
Virus Outbreak Filters rules      http://downloads.ironport.com/as
Feature Key updates               http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions     IronPort Servers
PXE Engine Updates                IronPort Servers
IronPort AsyncOS upgrades         IronPort Servers
IMS Secondary Service rules       IronPort Servers

Service (list):                   Update URL:

-------------------------------------------------------------------------------
McAfee Anti-Virus definitions     IronPort Servers
PXE Engine Updates                IronPort Servers
IronPort AsyncOS upgrades         IronPort Servers

Update intervals: 5m, 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
[]> setup

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

-------------------------------------------------------------------------------
Sophos Anti-Virus definitions     http://downloads.ironport.com/av
IronPort Anti-Spam rules          http://downloads.ironport.com/as
Intelligent Multi-Scan rules      http://downloads.ironport.com/as
Virus Outbreak Filters rules      http://downloads.ironport.com/as
Feature Key updates               http://downloads.ironport.com/asyncos

1. Use IronPort update servers (http://downloads.ironport.com)
```

Code Example 3-61 updateconfig

```
2. Use own server
[1]> 1

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

-------------------------------------------------------------------------------
McAfee Anti-Virus definitions      IronPort Servers
PXE Engine Updates                 IronPort Servers
IronPort AsyncOS upgrades          IronPort Servers

1. Use IronPort update servers
2. Use own server
[1]> 1

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

-------------------------------------------------------------------------------
IMS Secondary Service rules        IronPort Servers

1. Use IronPort update servers
2. Use own server
[1]> 1

For the following services, please select where the system will download the
list of available updates from:
Service (list):                    Update URL:

-------------------------------------------------------------------------------
McAfee Anti-Virus definitions      IronPort Servers
PXE Engine Updates                 IronPort Servers
IronPort AsyncOS upgrades          IronPort Servers

1. Use IronPort update servers
2. Use own update list
[1]> 2

Enter the full HTTP URL of the update list using the format
(http://optionalname:password@local.server:port/directory/manifest.xml). The
default HTTP port is 80; you do not need to specify the port unless you wish
to use a non-standard port. The optional username/password will be presented
using HTTP BASIC_AUTH. Leave the entry blank to use the default server.
```

Code Example 3-61 updateconfig

```
[]> enter the full path to the update list
```

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

Code Example 3-62 `version`

```
mail3.example.com> version

Current Version
===============
Model: C60
Version: 4.5.0-316
Build Date: 2005-04-13
Install Date: 2005-04-14 13:32:20
Serial #: XXXXXXXXXXX-XXXXXXX
BIOS: A15I
RAID: 2.7-1 3170
RAID Status: Okay
RAID Type: 10
mail3.example.com>
```

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.

Code Example 3-63 upgrade

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

Code Example 3-63 upgrade (Continued)

```
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

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 IronPort 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.

Code Example 3-64 `ldapconfig - New Server Profile`

```
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.
```

Code Example 3-64 `ldapconfig - New Server Profile` (Continued)

```
[]> new

Please create a name for this server configuration (Ex: "PublicLDAP"):
[]> PublicLDAP

Please enter the hostname:
[]> myldapserver.example.com

Use SSL to connect to the LDAP server? [N]> n

Select the authentication method to use for this server configuration:
1. Anonymous
2. Password based
[1]> 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.
```

Code Example 3-64 `ldapconfig - New Server Profile` (Continued)

```
- 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.
[]> 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.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> ldaprouting

Please create a name for this query:
[PublicLDAP.routing]> PublicLDAP.routing

Enter the LDAP query string:
[(mailLocalAddress={a})]> (mailLocalAddress={a})
```

Code Example 3-64 `ldapconfig - New Server Profile` (Continued)

```
Do you want to rewrite the Envelope Header? [N]> y

Enter the attribute which contains the full rfc822 email address for
the recipients.
[]> mailRoutingAddress

Do you want to send the messages to an alternate mail host? [N]> y

Enter the attribute which contains the alternate mailhost for the
recipients.
[]> mailForwardingAddress

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.
```

Code Example 3-64 `ldapconfig - New Server Profile` (Continued)

```
[]> 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})]> (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
```

Code Example 3-64 `ldapconfig - New Server Profile` (Continued)

```
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.

Code Example 3-65 ldapconfig - Configuring Global Settings

```
mail3.example.com> ldapconfig

No LDAP server configurations.


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

Choose the IP interface for LDAP traffic.
1. Auto
2. Management (10.92.145.175/24: esx16-esa01.qa)
[1]> 1

LDAP will determine the interface automatically.

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

The "Demo" certificate is currently configured. You may use "Demo", but this
will not be secure.


1. partner.com
2. Demo
Please choose the certificate to apply:
[1]> 1

No LDAP server configurations.


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

ldapflush

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

Code Example 3-66 `ldapflush`

```
mail3.example.com> ldapflush

Are you sure you want to flush any cached LDAP results? [N]> y

Flushing cache
mail3.example.com>
```

ldaptest

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.

Code Example 3-67 `ldaptest`

```
mail3.example.com> ldaptest

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

LDAP query test results:

               Query: PublicLDAP.ldapaccept
            Argument: admin@example.com
              Action: pass
```

Code Example 3-67 `ldaptest` (Continued)

```
LDAP query test finished.
mail3.example.com> ldaptest

Select which LDAP query to test:
1. PublicLDAP.ldapaccep
[1]> 1
Address to use in query:
[]> bogus@example.com

LDAP query test results:

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

MAIL DELIVERY CONFIGURATION/MONITORING

This section contains the following CLI commands:

- aliasconfig
- archivemessage
- altsrchost
- bounceconfig
- bouncerecipients
- bvconfig
- deleterecipients
- deliveryconfig
- delivernow
- destconfig
- hostrate
- hoststatus
- oldmessage
- rate
- resetcounters
- removemessage
- showmessage
- status
- tophosts
- topin
- unsubscribe
- workqueue

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 IronPort appliance:

```
aliasconfig export <filename>
```

Example

Code Example 3-68 `aliasconfig`

```
mail3.example.com> aliasconfig

No aliases in table.

Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import aliases from a file.
[]> new

How do you want your aliases to apply?

1. Globally
2. Add a new domain context
[1]> 2

Enter new domain context.
Separate multiple domains with commas.
Partial domains such as .example.com are allowed.
[]> example.com

Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
    - "user" - This user in this domain context.
    - "user@domain" - This email address.
[]> customercare

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.
```

Code Example 3-68 `aliasconfig` (Continued)

```
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> new

How do you want your aliases to apply?

1. Globally
2. Add a new domain context
3. example.com
[1]> 1

Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
    - "user@domain" - This email address.
    - "user" - This user for any domain
    - "@domain" - All users in this domain.
    - "@.partialdomain" - All users in this domain, or any of its sub
domains.
[]> admin

Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com

Adding alias admin: administrator@example.com
Do you want to add another alias?  [N]> n


There are currently 2 mappings defined.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> print

admin: administrator@example.com

[ example.com ]
customercare: bob@example.com, frank@example.com, sally@example.com
```

Code Example 3-68 `aliasconfig` (Continued)

```
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 3-3 Arguments for Configuring Aliases

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

archivemessage

Description

Archive older messages in your queue.

Usage

Commit: This command does not require a commit.

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

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

Example

In the following example, an older message is archived:

Code Example 3-69 `archivemessage`

```
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 (for example, the marketing campaign messaging system) is mapped to the AnotherPublicNet interface.

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

Code Example 3-70 `altsrchost`

```
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
```

Code Example 3-70 `altsrchost` (Continued)

```
Enter the Envelope From address or client IP address for which you want
to set up a Virtual Gateway mapping.  Partial addresses such as
"@example.com" or "user@" are allowed.
[]> @exchange.example.com

Which interface do you want to send messages for @exchange.example.com
from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 4

Mapping for @exchange.example.com on interface PublicNet created.

Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> new

Enter the Envelope From address or client IP address for which you want
to set up a Virtual Gateway mapping.  Partial addresses such as
"@example.com" or "user@" are allowed.
[]> 192.168.35.35

Which interface do you want to send messages for 192.168.35.35 from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 1

Mapping for 192.168.35.35 on interface AnotherPublicNet created.

Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
```

Code Example 3-70 `altsrchost` (Continued)

```
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> print

1. 192.168.35.35 -> AnotherPublicNet
2. @exchange.example.com -> PublicNet

Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]>
mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added 2 altsrchost mappings
Changes committed: Thu Mar 27 14:57:56 2003
```

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

Code Example 3-71 `bounceconfig`- Creating a Bounce Profile

```
mail3.example.com> bounceconfig

Current bounce profiles:
```

Code Example 3-71 `bounceconfig`- Creating a Bounce Profile

```
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
```

Code Example 3-71 `bounceconfig`- Creating a Bounce Profile

```
Please enter the email address to send hard bounce and delay warning.
[]> 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.
[]>
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):

Code Example 3-72 `bounceconfig`- Editing a Bounce Profile

```
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.
[]> edit

Please enter the number of the profile to edit:
[]> 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.
```

Code Example 3-72 `bounceconfig`- Editing a Bounce Profile

```
[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]>

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.

Code Example 3-73 `listenerconfig and bounceconfig` - Applying a Bounce Profile to a Listener

```
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
```

Code Example 3-73 `listenerconfig and bounceconfig` - Applying a Bounce Profile to a Listener (Continued)

```
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
```

Code Example 3-73 `listenerconfig and bounceconfig` - Applying a Bounce Profile to a Listener (Continued)

```
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: bouncepr1
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected
on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>

Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Enabled the bouncepr1 profile to the Outbound mail listener

Changes committed: Thu Mar 27 14:57:56 2003
```

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

Code Example 3-74 `bouncerecipients` - Bouncing Recipients by 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

Code Example 3-75 `boundcerecipients` - Bouncing Recipients by 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
```

Code Example 3-75 `boundcerecipients` - Bouncing Recipients by Address (Continued)

```
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

Code Example 3-76 `bouncerecipients` - bouncing All Recipients

```
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.

Code Example 3-77 `bvconfig`

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

Code Example 3-77 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
```

Code Example 3-77 bvconfig

```
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

Changes committed: Wed May 31 23:24:09 2006 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 IronPort 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

Code Example 3-78 `deleterecipients` - Delete Messages by Recipient Domain

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

Code Example 3-78 `deleterecipients` - Delete Messages by Recipient Domain (Continued)

```
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

Code Example 3-79 `deleterecipients` -Delete Messages 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

Code Example 3-80 `deleterecipients` - Delete all Message from a Queue

```
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.

Code Example 3-81 `deliveryconfig`

```
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
```

Code Example 3-81 `deliveryconfig` (Continued)

```
Enable "Possible Delivery" (recommended)?  [Y]> y

Please enter the default system wide maximum outbound message delivery
concurrency
[10000]> 9000

mail3.example.com>
```

delivernow

Description

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

Usage

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

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Code Example 3-82 `delivernow`

```
mail3.example.com> delivernow

Please choose an option for scheduling immediate delivery.
1. By recipient host
2. All messages
[1]> 1

Please enter the domain to schedule for immediate delivery.
[]>foo.com

Rescheduling all messages to foo.com for immediate 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 3-4 `destconfig` Subcommands

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

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

- Domain (recipient host)
- Maximum simultaneous connections to the domain
- Messages-per-connection limit
- Recipient limit
- System-wide or Virtual Gateway switch
- Enforce limits per 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 3-5 Example Destination Control Table Entries

Domain	Conn. Limit	Rcpt. Limit	Min. Prd.	Enforce MX/DOM
(default)	500	None	1	Domain
Unlisted domains get their own set of 500 connections with unlimited rcpts/hr				
(default)	500	None	1	MXIP
Mail gateways at unlisted domains get up to 500 connections, with unlimited rcpts/hr				
partner.com	10	500	60	Domain
All gateways at partner.com will share 10 connections, with 500 rcpts/minute maximum				
101.202.101.2	500	None	0	MXIP
Specifying an IP address				

Batch Format

The batch format of the `destconfig` command can be used to perform all the fuctions 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

Code Example 3-83 `destconfig` example: Configuring the Destination Configuration Table

```
mail3.example.com> destconfig

There are currently 2 entries configured.

Choose the operation you want to perform:
```

Code Example 3-83 `destconfig` example: Configuring the Destination Configuration Table

```
- 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

l
           Rate                Bounce        Bounce
Domain     Limiting  TLS       Verification  Profile
=========  ========  =======   ============  =========
(Default)  On        Off       Off           (Default)


Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.

[]> partner.com

Do you wish to configure a concurrency limit for partner.com? [Y]> y

Enter the max concurrency limit for "partner.com".
[500]> 100

Do you wish to apply a messages-per-connection limit to this domain?
[N]> n

Do you wish to apply a recipient limit to this domain? [N]> y
```

Code Example 3-83 `destconfig` example: Configuring the Destination Configuration Table

```
Enter the number of minutes used to measure the recipient limit.
[60]> 60

Enter the max number of recipients per 60 minutes for "partner.com".
[]> 50

Select how you want to apply the limits for partner.com:
1. One limit applies to the entire domain for partner.com
2. Separate limit for each mail exchanger IP address
[1]> 1

Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1

Do you wish to apply a specific TLS setting for this domain? [N]> n

Do you wish to apply a specific bounce verification address tagging
setting for
this domain? [N]> n

Do you wish to apply a specific bounce profile to this domain? [N]> n


There are currently 3 entries configured.

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Throttled delivery to partner.com in the destconfig table

Changes committed: Wed May 31 21:30:47 2006 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 118) configured to be used for all email delivery to the domain `newpartner.com`.

Code Example 3-84 `destconfig` example: Configuring Bounce Profile and TLS Settings

```
mail3.example.com> destconfig

There is currently 1 entry configured.
```

Code Example 3-84 `destconfig` example: Configuring Bounce Profile and TLS Settings

```
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:
```

Code Example 3-84 `destconfig` example: Configuring Bounce Profile and TLS Settings

```
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.
[]> detail

                Rate                Bounce        Bounce
Domain          Limiting  TLS       Verification  Profile
==============  ========  =======   ============  =========
newpartner.com  Default   Req       On            Default
(Default)       On        Off       Off           (Default)

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

newpartner.com
 Maximum messages per connection: Default
 Rate Limiting: Default
 TLS: Required
 Bounce Verification Tagging: On
 Bounce Profile: Default

Default
 Rate Limiting:
 500 concurrent connections
 No recipient limit
 Limits applied to entire domain, across all virtual gateways
 TLS: Off
 Bounce Verification Tagging: Off

There are currently 2 entries configured.
```

Code Example 3-84 `destconfig` example: Configuring Bounce Profile and TLS Settings

```
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> enabled TLS for delivery to newpartner.com using demo certificate

Changes committed: Wed May 31 22:05:57 2006 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 IronPort 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:

Code Example 3-85 `destconfig` example: Inbound "Shock Absorber"

```
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
```

Code Example 3-85 `destconfig` example: Inbound "Shock Absorber"

```
Do you wish to apply a recipient limit to this domain? [N]> y

Enter the number of minutes used to measure the recipient limit.
[60]> 1

Enter the max number of recipients per 1 minutes for
"exchange.example.com".
[]> 1000

Select how you want to apply the limits for exchange.example.com:
1. One limit applies to the entire domain for exchange.example.com
2. Separate limit for each mail exchanger IP address
[1]> 1

Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1

Do you wish to apply a specific TLS setting for this domain? [N]> n
Do you wish to apply a specific bounce verification address tagging
setting for this domain? [N]> n

Do you wish to apply a specific bounce profile to this domain? [N]> n

There are currently 3 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> set up shock absorber for inbound mail
```

Code Example 3-85 `destconfig` example: Inbound “Shock Absorber”

```
Changes committed: Wed May 31 22:25:28 2006 GMT

mail3.example.com>
```

Example: Global Settings

In this example, the TLS alert and certificate for TLS connections are configured.

Code Example 3-86 destconfig - Global Settings

```
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> setup

The "Demo" certificate is currently configured. You may use "Demo", but
this will not be secure.

1. partner.com
2. Demo
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

Code Example 3-87 hostrate

```
mail3.example.com> hostrate

Recipient host:
[]> aol.com

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

    Time      Host  CrtCncOut   ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt
              Status                      Delta   Delta     Delta     Delta
23:38:23        up          1         0       0       4         0         0
23:38:24        up          1         0       0       4         0         0
23:38:25        up          1         0       0      12         0         0
^C
```

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

Code Example 3-88 `hoststatus`

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com

Host mail status for: 'aol.com'
Status as of:         Fri Aug  8 11:12:00 2003
Host up/down:         up

Counters:
  Queue
    Soft Bounced Events                       0
  Completion
    Completed Recipients                      1
      Hard Bounced Recipients                 1
        DNS Hard Bounces                      0
        5XX Hard Bounces                      1
        Filter Hard Bounces                   0
        Expired Hard Bounces                  0
        Other Hard Bounces                    0
      Delivered Recipients                    0
      Deleted Recipients                      0

Gauges:
  Queue
    Active Recipients                         0
      Unattempted Recipients                  0
      Attempted Recipients                    0
    Connections
      Current Outbound Connections            0
      Pending Outbound Connections            0

Oldest Message        No Messages
Last Activity         Fri Aug  8 11:04:24 2003
Ordered IP addresses: (expiring at Fri Aug  8 11:34:24 2003)
    Preference   IPs
    15           64.12.137.121    64.12.138.89     64.12.138.120
    15           64.12.137.89     64.12.138.152    152.163.224.122
    15           64.12.137.184    64.12.137.89     64.12.136.57
    15           64.12.138.57     64.12.136.153    205.188.156.122
    15           64.12.138.57     64.12.137.152    64.12.136.89
    15           64.12.138.89     205.188.156.154  64.12.138.152
    15           64.12.136.121    152.163.224.26   64.12.137.184
    15           64.12.138.120    64.12.137.152    64.12.137.121
```

Code Example 3-88 `hoststatus` (Continued)

```
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
```

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:

Code Example 3-89 oldmessage

```
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
```

Code Example 3-89 oldmessage (Continued)

```
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

Code Example 3-90 `rate`

```
mail3.example.com> rate

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

Hit Ctrl-C to return to the main prompt.

Time     Connections Recipients          Recipients              Queue
            In   Out   Received    Delta  Completed    Delta     K-Used
23:37:13    10     2   41708833        0   40842686        0         64
23:37:14     8     2   41708841        8   40842692        6        105
23:37:15     9     2   41708848        7   40842700        8         76
23:37:16     7     3   41708852        4   40842705        5         64
23:37:17     5     3   41708858        6   40842711        6         64
23:37:18     9     3   41708871       13   40842722       11         67
23:37:19     7     3   41708881       10   40842734       12         64
23:37:21    11     3   41708893       12   40842744       10         79
^C
```

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

Code Example 3-91 `resetcounters`

```
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

`Code Example 3-92 removemessage`

```
example.com> removemessage 1

MID 1: 19 secs old

Received: from example2.com ([172.16.0.102])
  by test02.com with SMTP; 01 Mar 2007 19:50:41 -0800
From: user123@test02.com
To: 9526@example.com
Subject: Testing
Message-Id: <20070302035041.67424.53212@test02.com>

Remove this message? [N]> y
```

showmessage

Description

Shows the message and message body for a specified message ID.

Usage

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

Cluster Management: This command is restricted to machine mode.

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

Example

Code Example 3-93 `showmessage`

```
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.
```

status

The status command is used to display the system status of your IronPort 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

Code Example 3-94 `status`

```
example.mail3.com> status

Enter "status detail" for more information.

Status as of:                  Tue Aug 02 14:03:53 2005 PDT
Up since:                      Tue Aug 02 10:27:22 2005 PDT (3h 36m 31s)
Last counter reset:            Tue Aug 02 10:24:51 2005 PDT
System status:                 Online
Oldest Message:                No Messages
Feature - IronPort Anti-Spam:  25 days
Feature - Receiving:           25 days
```

Code Example 3-94 `status` (Continued)

```
Feature - Sophos:              25 days
Feature - Virus Outbreak Filters: 25 days
Feature - Central Mgmt:        29 days

Counters:                               Reset          Uptime        Lifetime
  Receiving
    Messages Received                       0               0               2
    Recipients Received                     0               0               2
  Rejection
    Rejected Recipients                     1               1               1
    Dropped Messages                        0               0               0
  Queue
    Soft Bounced Events                     0               0               0
  Completion
    Completed Recipients                    0               0               2
  Current IDs
    Message ID (MID)                                                        3
    Injection Conn. ID (ICID)                                               1
    Delivery Conn. ID (DCID)                                                1

Gauges:                                Current
  Connections
    Current Inbound Conn.                   0
    Current Outbound Conn.                  0
  Queue
    Active Recipients                       0
    Messages In Work Queue                  0
    Messages In Quarantine                  0
    Kilobytes Used                          0
      Kilobytes In Quarantine               0
    Kilobytes Free                 39,845,888
```

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

Code Example 3-95 `tophosts`

```
mail3.example.com> tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
5. Hard Bounced Recipients
[1]> 1

Status as of:         Mon Nov 18 22:22:23 2003
Active Conn. Deliv. Soft  Hard
# Recipient Host Recip Out Recip. Bounced Bounced
1  aol.com 365 10 255 21 8
2  hotmail.com 290 7 198 28 13
3  yahoo.com 134 6 123 11 19
4  excite.com 98 3 84 9 4
5  msn.com 84 2 76 33 29
mail3.example.com>
```

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

Code Example 3-96 `topin`

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003

#Remote hostname            Remote IP addr.   listener        Conn. In
1mail.remotedomain01.com    172.16.0.2        Incoming01           10
2mail.remotedomain01.com    172.16.0.2        Incoming02           10
3mail.remotedomain03.com    172.16.0.4        Incoming01            5
```

Code Example 3-96 `topin` (Continued)

```
4mail.remotedomain04.com    172.16.0.5        Incoming02              4
5mail.remotedomain05.com    172.16.0.6        Incoming01              3

6mail.remotedomain06.com    172.16.0.7        Incoming02              3
7mail.remotedomain07.com    172.16.0.8        Incoming01              3
8mail.remotedomain08.com    172.16.0.9        Incoming01              3
9mail.remotedomain09.com    172.16.0.10       Incoming01              3
10mail.remotedomain10.com    172.16.0.11       Incoming01             2

11mail.remotedomain11.com    172.16.0.12       Incoming01             2
12mail.remotedomain12.com    172.16.0.13       Incoming02             2
13mail.remotedomain13.com    172.16.0.14       Incoming01             2
14mail.remotedomain14.com    172.16.0.15       Incoming01             2
15mail.remotedomain15.com    172.16.0.16       Incoming01             2

16mail.remotedomain16.com    172.16.0.17       Incoming01             2
17mail.remotedomain17.com    172.16.0.18       Incoming01             1
18mail.remotedomain18.com    172.16.0.19       Incoming02             1
19mail.remotedomain19.com    172.16.0.20       Incoming01             1
20mail.remotedomain20.com    172.16.0.21       Incoming01             1
```

unsubscribe

Description

Update the global unsubscribe list

Usage

Commit: This command requires a 'commit'.

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

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

Example

In this example, the address `user@example.net` is added to the Global Unsubscribe list, and the feature is configured to hard bounce messages. Messages sent to this address will be bounced; the appliance will bounce the message immediately prior to delivery.

Code Example 3-97 `unsubscribe`

```
mail3.example.com> unsubscribe

Global Unsubscribe is enabled. Action: drop.

Choose the operation you want to perform:
- NEW - Create a new entry.
```

Code Example 3-97 `unsubscribe` (Continued)

```
- 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.

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup

Do you want to enable the Global Unsubscribe feature? [Y]> y

Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2

Global Unsubscribe is enabled. Action: bounce.

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Added username “user@example.net” to global unsubscribe
```

Code Example 3-97 `unsubscribe` (Continued)

```
Changes committed: Thu Mar 27 14:57:56 2003
```

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

Code Example 3-98 `workqueue` - Manually Pausing the Work Queue

```
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:

Code Example 3-99 `workqueue` - Resuming a Paused Work Queue

```
mail3.example.com> workqueue

Status:   Paused by admin: checking LDAP server
Messages: 1243

Resume the work queue?   [Y]> y

Status:   Operational
```

Code Example 3-99 `workqueue` - Resuming a Paused Work Queue (Continued)

```
Messages: 1243
```

NETWORKING CONFIGURATION / NETWORK TOOLS

This section contains the following CLI commands:

- etherconfig
- interfaceconfig
- netstat
- nslookup
- ping
- routeconfig
- setgateway
- sethostname
- smtproutes
- telnet
- traceroute

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 of Editing Media Settings

Code Example 3-100 `etherconfig` -Editing Media Settings

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]> media

Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
```

Code Example 3-100 `etherconfig` (Continued)-Editing Media Settings (Continued)

```
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]> edit

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

Please choose the Ethernet media options for the Data 2 interface.
1. Autoselect
2. 10baseT/UTP half-duplex
3. 10baseT/UTP full-duplex
4. 100baseTX half-duplex
5. 100baseTX full-duplex
6. 1000baseTX half-duplex
7. 1000baseTX full-duplex
[1]> 5

Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (100baseTX full-duplex: <100baseTX full-duplex>)
00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]>
```

Enabling NIC Pairing via the `etherconfig` Command

Code Example 3-101 `etherconfig` - Enabling NIC Pairing

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
```

Code Example 3-101 `etherconfig` - Enabling NIC Pairing (Continued)

```
[]> pairing

Paired interfaces:

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

Please enter a name for this pair (Ex: "Pair 1"):
[]> Pair 1

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

Paired interfaces:
1. Pair 1:
 Primary (Data 1) Active, Link is up
 Backup (Data 2) Standby, Link is up

Choose the operation you want to perform:
- FAILOVER - Manually failover to other port.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
```

Using the `failover` Subcommand for NIC Pairing

In this example, a manual failover is issued, forcing the Data 2 interface to become the primary interface. Note that you must issue the `status` sub-command to see the change in the CLI.

Code Example 3-102 `etherconfig` - Issuing a Manual Failover Command

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]> pairing

Paired interfaces:
1. Pair 1:
```

Code Example 3-102 `etherconfig` - Issuing a Manual Failover Command (Continued)

```
 Primary (Data 1) Active, Link is up
 Backup (Data 2) Standby, Link is up

Choose the operation you want to perform:
- FAILOVER - Manually failover to other port.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]> failover

Paired interfaces:
1. Pair 1:
        Primary (Data 1) Active, Link is up
        Backup (Data 2) Standby, Link is up

Choose the operation you want to perform:
- FAILOVER - Manually failover to other port.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]> status

Paired interfaces:
1. Pair 1:
        Primary (Data 1) Standby, Link is up
        Backup (Data 2) Active, Link is up
Choose the operation you want to perform:
- FAILOVER - Manually failover to other port.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]>
```

Creating a New VLAN via the `etherconfig` Command

In this example, two VLANs are created (named VLAN 31 and VLAN 34) on the Data 1 port:

Code Example 3-103 `etherconfig` - Creating a New VLAN

```
mail3.example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
```

Code Example 3-103 `etherconfig` - Creating a New VLAN (Continued)

```
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]> vlan

VLAN interfaces:

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

VLAN tag ID for the interface (Ex: "34"):
[]> 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   34 (Data 1)

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

VLAN tag ID for the interface (Ex: "34"):
[]> 31

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   31 (Data 1)
2. VLAN   34 (Data 1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
```

Code Example 3-103 `etherconfig` - Creating a New VLAN (Continued)

```
[]>

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]>
```

Enabling the Loopback Interface via the `etherconfig` Command

Once enabled, the loopback interface is treated like any other interface (e.g. Data 1):

Code Example 3-104 `etherconfig` Enabling the Loopback Interface

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]> loopback

Currently configured loopback interface:

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

Currently configured loopback interface:
1. Loopback

Choose the operation you want to perform:
- DISABLE - Disable Loopback Interface.
[]>

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]>
```

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 fuctions of the traditional CLI command.

- Creating a new interface

```
interfaceconfig new <name>
                   <ip address>
                   <ethernet interface>
                   <netmask>
                   <hostname>
                   [--ftp]
                   [--telnet]
                   [--ssh]
                   [--http]
```

- Deleting an interface

```
interfaceconfig delete <name>
```

Example: Configuring an Interface

Code Example 3-105 `interfaceconfig` Configuring an Interface

```
mail3.example.com> interfaceconfig

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: 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.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Data 1]>

IP Address (Ex: 192.168.1.2):
[192.168.1.1]>

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

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>

Hostname:
[mail3.example.com]>

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

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

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

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

Which port do you want to use for HTTP?
```

Code Example 3-105 `interfaceconfig` Configuring an Interface (Continued)

```
[80]> 80

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

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

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

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

You have not entered a certificate. To assure privacy, run
'certconfig' first.  You may use the demo certificate
to test HTTPS, but this will not be secure.
Do you really wish to use a demo certificate?  [Y]> y

Both HTTP and HTTPS are enabled for this interface, should HTTP
requests redirect to the secure service?  [Y]>

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data 1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data 2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: 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.
[]>
mail3.example.com> commit

Please enter some comments describing your changes:
[]> enabled HTTP, HTTPS for Data 1

Changes committed: Mon Jul  7 13:21:23 2003
mail3.example.com>
```

Example: Changing the IronPort Spam Quarantine URL

The following example shows a change in the IronPort Spam Quarantine URL.

Code Example 3-106 Changing the IronPort Spam Quarantine URL

```
mail3.example.com]>interfaceconfig

Currently configured interfaces:
```

Code Example 3-106 Changing the IronPort Spam Quarantine URL (Continued)

```
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: 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.
[]> edit

Enter the number of the interface you wish to edit.
[]> 3

IP interface name (Ex: "InternalNet"):
[Management]>
Which port do you want to use for HTTP?
[80]>
[ ... ]
Do you want to enable IronPort Spam Quarantine HTTP on this interface?
[Y]>

Which port do you want to use for IronPort Spam Quarantine HTTP?
[82]>

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

Which port do you want to use for IronPort Spam Quarantine HTTPS?
[83]>

You have not entered an HTTPS certificate.  To assure privacy, run
"certconfig" first.
You may use the demo, but this will not be secure.
Do you really wish to use a demo certificate? [Y]>

Both HTTP and HTTPS are enabled for this interface, should HTTP
requests redirect to the secure service? [Y]>


Both IronPort Spam Quarantine HTTP and IronPort Spam Quarantine HTTPS
are enabled for this interface, should IronPort Spam Quarantine HTTP
requests redirect to the secure service? [Y]>
```

Code Example 3-106 Changing the IronPort Spam Quarantine URL (Continued)

```
Do you want Management as the default interface for IronPort Spam
Quarantine? [Y]>

Do you want to use a custom base URL in your IronPort Spam Quarantine
email notifications? [N]> y

Enter the custom base URL (Ex: "http://isq.example.url:81/")

[]> http://ISQ.example.com:82/

You have edited the interface you are currently logged into. Are you
sure you want to change it? [Y]> y

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: 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.
```

nslookup

Description

Use the `nslookup` command to check the DNS functionality.

The `nslookup` 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 3-6 `nslookup` Command Query Types

Query Type	Description
A	the host's Internet address
CNAME	the canonical name for an alias
MX	the mail exchanger
NS	the name server for the named zone
PTR	the hostname if the query is an Internet address, otherwise the pointer to other information

Table 3-6 `nslookup` Command Query Types

Query Type	Description
SOA	the domain's "start-of-authority" information
TXT	the text information

netstat

Description

Use the `netstat` command to displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. Note that this version will not support all arguments. Specifically, you cannot use -a, -A, -g, -m, -M, -N, -s. The command was designed to be run in interactive mode, so that you may enter netstat, then choose from five options to report on. You can also specify the interface to listen on and the interval for display.

Usage

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

Cluster Management: This command is restricted to machine mode.

Batch Command: This command does not support a batch format

Example

Code Example 3-107 `netstat`

```
example.com> netstat
Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
[1]> 2
Select the ethernet interface whose state you wish to display:
1. Data 1
2. Data 2
3. Management
4. ALL
[]> 1
Show the number of bytes in and out? [N]>
Show the number of dropped packets? [N]> y
Name    Mtu Network       Address              Ipkts Ierrs    Opkts
Oerrs  Coll Drop
Data 1 1500 197.19.1/24   example.com       30536     -        5     -
-    -
```

Code Example 3-107 `netstat` (Continued)

```
example.com>
```

ping

Description

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

Code Example 3-108 `ping`

```
mail3.example.com> ping

Which interface do you want to send the pings from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1

Please enter the host you wish to ping.
[]> anotherhost.example.com


Press Ctrl-C to stop.
PING anotherhost.example.com (x.x.x.x): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=0 ttl=64 time=1.421 ms
64 bytes from 10.19.0.31: icmp_seq=1 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=2 ttl=64 time=0.118 ms
64 bytes from 10.19.0.31: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 10.19.0.31: icmp_seq=4 ttl=64 time=0.139 ms
64 bytes from 10.19.0.31: icmp_seq=5 ttl=64 time=0.125 ms
64 bytes from 10.19.0.31: icmp_seq=6 ttl=64 time=0.124 ms
64 bytes from 10.19.0.31: icmp_seq=7 ttl=64 time=0.122 ms
64 bytes from 10.19.0.31: icmp_seq=8 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
```

Code Example 3-108 `ping` (Continued)

```
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
^C
```

Note — You must use Control-C to end the `ping` command.

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, IronPort 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`.

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 does not support a batch format.

Example

Code Example 3-109 `routeconfig`

```
mail3.example.com> routeconfig

Currently configured routes:
1. WestNet Destination: 192.168.11.0/24 Gateway: 192.168.14.2
2. EastNet Destination: 192.168.13.0/24 Gateway: 192.168.14.3

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

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

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

Gateway address for traffic to 192.168.12.0/24:
[]> 192.168.14.4
Currently configured routes:
1. WestNet Destination: 192.168.11.0/24 Gateway: 192.168.14.2
2. EastNet Destination: 192.168.13.0/24 Gateway: 192.168.14.3
3. EuropeNet Destination: 192.168.12.0/24 Gateway: 192.168.14.4

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

mail3.example.com> commit

Please enter some comments describing your changes:
[]> Created new static route
Changes committed: Mon Jan 01 12:00:01 2003
```

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

Code Example 3-110 `setgateway`

```
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
Changes committed: Mon Jan 01 12:00:01 2003
```

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 IronPort 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

Code Example 3-111 `sethostname`

```
oldname.example.com> sethostname

[oldname.example.com]> mail3.example.com

oldname.example.com>
```

For the hostname change to take effect, you must enter the `commit` command. After you have successfully committed the hostname change, the new name appears in the CLI prompt:

Code Example 3-112

```
oldname.example.com> commit

Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Apr 18 12:00:01 2003
```

The new hostname appears in the prompt as follows:

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

smtproutes

Description

Set up permanent domain redirections.

Usage

Commit: This command requires a 'commit'.

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

Batch Command: This command supports a batch format.

Batch Format

The batch format of the `smtproutes` command can be used to perform all the fuctions 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 `smptroutes` 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.)

`Code Example 3-113 smtproutes`

```
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.
```

Code Example 3-113 smtproutes

```
[]> relay1.example.com/pri=10, relay2.example.com, backup-
relay.example.com

Mapping for example.com to relay1.example.com, relay2.example.com,
backup-relay.example.com/pri=10 created.

There are currently 1 routes configured.

Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.
[]>
```

Use `smtproutes -> EDIT` to modify the domain for an SMTP route.

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

Code Example 3-114 `telnet`

```
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 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

Code Example 3-115 `traceroutes`

```
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
```

Code Example 3-115 `traceroutes` (Continued)

```
Please enter the host to which you want to trace the route.
[]> 10.1.1.1

Press Ctrl-C to stop.
traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets
 1  gateway (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms
 2  hostname (10.1.1.1)  0.298 ms  0.302 ms  0.291 ms
mail3.example.com>
```

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.

Code Example 3-116 `dictionaryconfig` - Creating a Dictionary 1

```
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]>
```

Code Example 3-116 `dictionaryconfig` - Creating a Dictionary 1 (Continued)

```
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.
[]>
```

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.

Code Example 3-117 `dictionaryconfig` - Creating a Dictionary 2

```
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
```

Code Example 3-117 `dictionaryconfig` - Creating a Dictionary 2 (Continued)

```
Currently configured content dictionaries:
1. secret_words

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

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

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

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

Enter the default encoding to be used for exporting this dictionary:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[2]>

Choose the operation you want to perform on dictionary 'secret_words':
```

Code Example 3-117 `dictionaryconfig` - Creating a Dictionary 2 (Continued)

```
- 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

Changes committed: Thu Feb 03 13:00:19 2005 PST
mail3.example.com>
```

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`.

Code Example 3-118 `dictionaryconfig` - Importing Dictionaries

```
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
```

Code Example 3-118 `dictionaryconfig` - Importing Dictionaries (Continued)

```
Enter the name of the file to import:
[]> profanity.txt

Enter the encoding to use for the imported file:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[2]>

84 entries imported successfully.
Currently configured content dictionaries:
1. profanity

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]>
mail3.example.com> commit
```

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`

Code Example 3-119 `dictionaryconfig` - Exporting a Dictionary

```
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.
```

Code Example 3-119 `dictionaryconfig` - Exporting a Dictionary (Continued)

```
- RENAME - Change the name of a content dictionary.
[]> edit

Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1

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

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

mail3.example.com> dictionaryconfig

Currently configured content dictionaries:
1. secret_words

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

Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1

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

Enter a name for the exported file:
```

Code Example 3-119 `dictionaryconfig` - Exporting a Dictionary (Continued)

```
[]> secret_words_export.txt
```

exceptionconfig

Description

Use the `exceptionconfig` command in the CLI to create the domain exception table. In this example, the email address "admin@zzzaaazzz.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

Code Example 3-120 `exceptionconfig`

```
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.

Code Example 3-121 `filters`

```
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.
```

Code Example 3-121 `filters` (Continued)

```
- 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.

Example

In this example, the `policyconfig -> edit -> antispam` subcommand is used to edit the IronPort 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 IronPort 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.
- Unwanted marketing messages are delivered with the text `[MARKETING]` prepended to the subject line.

Finally, the changes are committed.

Note — See Table 3-127 on page 208 to see an example of how DLP policies are enabled on an outgoing mail policy.

`Code Example 3-122 policyconfig` - Editing the Default Anti-Spam Settings

```
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: Content Filter: VOF:
-----           ------------  ----------- --------------- -------
```

Code Example 3-122 `policyconfig` - Editing the Default Anti-Spam Settings

```
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit

   Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
   -----           -------------  ----------- --------------- -------

1. DEFAULT         IronPort       McAfee      Off             Enabled

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

Policy Summaries:

Anti-Spam: IronPort - Deliver, Prepend "[SPAM] " to Subject
Suspect-Spam: IronPort - Deliver, Prepend "[SUSPECTED SPAM] " to Subject
Anti-Virus: McAfee - Scan and Clean
Content Filters: Off (No content filters have been created)
Virus Outbreak Filters: Enabled. No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
[]> antispam


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

Begin Anti-Spam configuration

Some messages will be positively identified as spam.  Some messages will be
identified as suspected spam. You can set the IronPort Anti-Spam Suspected
Spam Threshold below.
The following configuration options apply to messages POSITIVELY identified
as spam:
```

Code Example 3-122 `policyconfig` - Editing the Default Anti-Spam Settings

```
What score would you like to set for the IronPort Anti-Spam spam threshold?
[90]> 90

1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as spam?
[1]> 2

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

Do you want to enable special treatment of suspected spam? [Y]> y

What score would you like to set for the IronPort Anti-Spam suspect spam
threshold?
[50]> 50

The following configuration options apply to messages identified as SUSPECTED
spam:
1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as SUSPECTED spam?
[1]> 4

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

1. PREPEND
2. APPEND
3. NONE
Do you want to add text to the subject of messages identified as SUSPECTED
spam?
[1]> 1

What text do you want to prepend to the subject?
[[SUSPECTED SPAM] ]> [quarantined: possible spam]

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

Enter the name of the header:
[]> X-quarantined
```

Code Example 3-122 `policyconfig` - Editing the Default Anti-Spam Settings

```
Enter the text for the content of the header:
[]> true

Marketing email is normally legitimate email but sometimes undesirable. Do
you want to enable special treatment of marketing messages? [N]> y

The following configuration options apply to messages identified as marketing
messages:
1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as marketing messages?
[1]> 1

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

1. PREPEND
2. APPEND
3. NONE
Do you want to add text to the subject of messages identified as marketing
messages?
[1]> 1

What text do you want to prepend to the subject?
[[MARKETING] ]> [MARKETING]

Do you want marketing messages sent to an external quarantine or alternate
destination host? [N]> n

Do you want to add a custom header to messages identified as marketing
messages? [N]> n

Do you want marketing messages sent to an alternate envelope recipient? [N]> n

Anti-Spam configuration complete

Policy Summaries:

Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original
message.
Marketing-Messages: IronPort - Deliver, Prepend "[MARKETING]" to Subject
Anti-Virus: McAfee - Scan and Clean
Content Filters: Off (No content filters have been created)
```

Code Example 3-122 `policyconfig` - Editing the Default Anti-Spam Settings

```
Virus Outbreak Filters: Enabled. No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
[]>

Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> configured anti-spam for Incoming Default Policy

Changes committed: Tue Nov 17 22:00:35 2009 GMT
```

Then, use the new subcommand to add two new policies for different sets of users — the sales organization and the engineering organization — and configure different email security settings for each. In the CLI, you can configure different settings than the default as you create the policy.

First, create the policy for the sales team, specifying a more aggressive anti-spam setting:

Code Example 3-123 `policyconfig` - Creating a Policy for the Sales Team

```
Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
```

Code Example 3-123 policyconfig - Creating a Policy for the Sales Team

```
- FILTERS - Edit content filters
[]> new

Enter the name for this policy:
[]> sales_team

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

Enter a member for this policy:
[]> ldap(sales)

Please select an LDAP group query:
1. PublicLDAP.ldapgroup
[1]> 1

Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1

Add another member? [Y]> n

Would you like to enable Anti-Spam support? [Y]> y

Use the policy table default? [Y]> n

Begin Anti-Spam configuration

Some messages will be positively identified as spam.  Some messages will be
identified as suspected spam. You can set the IronPort Anti-Spam Suspected
Spam Threshold below.
The following configuration options apply to messages POSITIVELY identified
as spam:
What score would you like to set for the IronPort Anti-Spam spam threshold?
[90]> 90

1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as spam?
[1]> 2
```

Code Example 3-123 `policyconfig` - Creating a Policy for the Sales Team

```
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

Marketing email is normally legitimate email but sometimes undesirable. Do you
want to enable special treatment of marketing messages? [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 Virus Outbreak Filters for this policy? [Y]> y

Use the policy table default? [Y]> y

Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
```

Code Example 3-123 policyconfig - Creating a Policy for the Sales Team

```
sales_team      IronPort       Default     Default         Default
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

Then, create the policy for the engineering team (three individual email recipients), specifying that `.dwg` files are exempt from Virus Outbreak Filter scanning.

Code Example 3-124 policyconfig - Creating a Policy for the Engineering Team

```
Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> new

Enter the name for this policy:
[]> engineering

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

Enter a member for this policy:
```

Code Example 3-124 policyconfig - Creating a Policy for the Engineering Team

```
[]> 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 Virus 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
Virus Outbreak Filters? [N]> y
```

Code Example 3-124 policyconfig - Creating a Policy for the Engineering Team

```
Choose the operation you want to perform:
- NEW - Add a file extension
[]> new

Enter a file extension:
[]> dwg


Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]> print

The following file extensions will bypass Virus Outbreak Filter
processing:
dwg


Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]>

Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
engineering     Default        Default     Default         Enabled
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

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:

Code Example 3-125 `policyconfig` - Creating the `scan_for_confidential` Content Filter

```
Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
engineering     Default        Default     Default         Enabled
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> filters

No filters defined.

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

Enter a name for this filter:
[]> scan_for_confidential

Enter a description or comment for this filter (optional):
[]> scan all incoming mail for the string 'confidential'

Filter Name:  scan_for_confidential

Conditions:
Always Run

Actions:
No actions defined yet.
```

Code Example 3-125 `policyconfig` - Creating the `scan_for_confidential` Content 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
[]> 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. Envelope Recipient Address
13. Envelope Recipient in LDAP Group
14. Envelope Sender Address
15. Envelope Sender in LDAP Group
16. Reputation Score
17. Remote IP
18. DKIM authentication result
19. 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)
```

Code Example 3-125 `policyconfig` - Creating the `scan_for_confidential` Content Filter

```
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 Virus 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
```

Code Example 3-125 `policyconfig` - Creating the `scan_for_confidential` Content Filter

```
Enter the subject to use:
[$Subject]> [message matched confidential filter]

Do you want to edit the return path of the Bcc message? [N]> n

Filter Name:  scan_for_confidential

Conditions:
body-contains("confidential", 1)

Actions:
bcc ("hr@example.com", "[message matched confidential filter]")

Description:
scan all incoming mail for the string 'confidential'

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

1. Condition
2. Action
[1]> 2

1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
```

Code Example 3-125 `policyconfig` - Creating the `scan_for_confidential` Content Filter

```
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 Virus Outbreak Filters check
[1]> 14

1. Policy
[1]> 1

Filter Name:  scan_for_confidential

Conditions:
body-contains("confidential", 1)

Actions:
bcc ("hr@example.com", "[message matched confidential filter]")
quarantine ("Policy")

Description:
scan all incoming mail for the string 'confidential'

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- MOVE - Reorder the conditions or actions
- SAVE - Save filter
[]> save

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

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

Code Example 3-125 illustrates creating the next two content filters. (Note that you cannot specify the variables for envelope sender and envelope recipient from within the CLI.)

Code Example 3-126 `policyconfig` - 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
```

Code Example 3-126 `policyconfig` - Creating the `no_mp3s` and `ex_employee` Content Filters

```
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 Virus Outbreak Filters check
[1]> 12

Enter the file type to strip:
[]> mp3

Do you want to enter specific text to use in place of any stripped
attachments?[N]> n

Filter Name:  no_mp3s

Conditions:
Always Run

Actions:
drop-attachments-by-filetype("mp3")

Description:
strip all MP3 attachments

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- SAVE - Save filter
[]> save

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

Code Example 3-126 `policyconfig` - 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
- MOVE - Reorder a filter
- RENAME - Rename a filter
[]> new

Enter a name for this filter:
[]> ex_employee

Enter a description or comment for this filter (optional):
[]> bounce messages intended for Doug

Filter Name:  ex_employee

Conditions:
Always Run

Actions:
No actions defined yet.

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add

1. Condition
2. Action
[1]> 1

1. Message Body Contains
2. Only Body Contains (Attachments are not scanned)
3. Message Body Size
4. Subject Header
5. Other Header
6. Attachment Contains
7. Attachment File Type
8. Attachment Name
9. Attachment MIME Type
```

Code Example 3-126 `policyconfig` - Creating the `no_mp3s` and `ex_employee` Content Filters

```
10. Attachment Protected
11. Attachment Unprotected
12. Envelope Recipient Address
13. Envelope Recipient in LDAP Group
14. Envelope Sender Address
15. Envelope Sender in LDAP Group
16. Reputation Score
17. Remote IP
18. DKIM authentication result
19. SPF verification result
[1]> 12

Enter regular expression to search Recipient address for:
[]> doug

Filter Name:  ex_employee

Conditions:
rcpt-to == "doug"

Actions:
No actions defined yet.

Description:
bounce messages intended for Doug

Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[]> add

1. Condition
2. Action
[1]> 2

1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
```

Code Example 3-126 `policyconfig` - Creating the `no_mp3s` and `ex_employee` Content Filters

```
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 Virus Outbreak Filters check
[1]> 2

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

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

Enter the subject to use:
[]> message bounced for ex-employee of example.com

Do you want to edit the return path of the notification? [N]> n

Do you want to include a copy of the original message as an attachment to the
notification? [N]> y

Filter Name:  ex_employee

Conditions:
rcpt-to == "doug"

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

Description:
bounce messages intended for Doug

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

Code Example 3-126 `policyconfig` - Creating the `no_mp3s` and `ex_employee` Content Filters

```
- DELETE - Delete condition or action
- SAVE - Save filter
[]> add

1. Condition
2. Action
[1]> 2

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

Code Example 3-126 `policyconfig` - Creating the `no_mp3s` and `ex_employee` Content Filters

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

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

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

Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
engineering     Default        Default     Default         Enabled
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

Code Example 3-126 illustrates how to enable the policies once again to enable the content filters for some policies, but not for others.

Code Example 3-127 policyconfig 0 Enabling Content Filters for Specific Policies

```
Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           ------------   ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
engineering     Default        Default     Default         Enabled
DEFAULT         IronPort       McAfee      Off             Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> edit

   Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
   -----           ------------   ----------- --------------- -------

1. sales_team      IronPort       Default     Default         Default
2. engineering     Default        Default     Default         Enabled
3. DEFAULT         IronPort       McAfee      Off             Enabled

Enter the name or number of the entry you wish to edit:
[]> 3

Policy Summaries:

Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original
message.
Marketing-Messages: IronPort - Deliver, Prepend "[MARKETING]" to Subject
Anti-Virus: McAfee - Scan and Clean
Content Filters: Off
Virus Outbreak Filters: Enabled. No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
```

Code Example 3-127 policyconfig 0 Enabling Content Filters for Specific Policies (Continued)

```
- FILTERS - Modify filters
[]> filters


Choose the operation you want to perform:
- ENABLE - Enable Content Filters policy
[]> enable

1.        scan_for_confidential
2.        no_mp3s
3.        ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1

1. Active scan_for_confidential
2.        no_mp3s
3.        ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 2

1. Active scan_for_confidential
2. Active no_mp3s
3.        ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3

1. Active scan_for_confidential
2. Active no_mp3s
3. Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>

Policy Summaries:

Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original
message.
Marketing-Messages: IronPort - Deliver, Prepend "[MARKETING]" to Subject
Anti-Virus: McAfee - Scan and Clean
Content Filters: Enabled. Filters: scan_for_confidential, no_mp3s,
ex_employee
Virus Outbreak Filters: Enabled. No bypass extensions.

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
```

Code Example 3-127 policyconfig 0 Enabling Content Filters for Specific Policies (Continued)

```
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
- FILTERS - Modify filters
[]>

Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
engineering     Default        Default     Default         Enabled
DEFAULT         IronPort       McAfee      Enabled         Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> edit

   Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
   -----           -------------  ----------- --------------- -------

1. sales_team      IronPort       Default     Default         Default
2. engineering     Default        Default     Default         Enabled
3. DEFAULT         IronPort       McAfee      Enabled         Enabled

Enter the name or number of the entry you wish to edit:
[]> 2

Policy Summaries:

Anti-Spam: Default
Anti-Virus: Default
Content Filters: Default
Virus 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
```

Code Example 3-127 policyconfig 0 Enabling Content Filters for Specific Policies (Continued)

```
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
- FILTERS - Modify filters
[]> filters


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

1.        scan_for_confidential
2.        no_mp3s
3.        ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1

1. Active scan_for_confidential
2.        no_mp3s
3.        ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3

1. Active scan_for_confidential
2.        no_mp3s
3. Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>

Policy Summaries:

Anti-Spam: Default
Anti-Virus: Default
Content Filters: Enabled. Filters: scan_for_confidential, ex_employee
Virus 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
```

Code Example 3-127 policyconfig 0 Enabling Content Filters for Specific Policies (Continued)

```
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
- FILTERS - Modify filters
[]>

Incoming Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:
-----           -------------  ----------- --------------- -------
sales_team      IronPort       Default     Default         Default
engineering     Default        Default     Enabled         Enabled
DEFAULT         IronPort       McAfee      Enabled         Enabled


Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```

Note — The CLI does not contain the notion of adding a new content filter within an individual policy. Rather, the `filters` subcommand forces you to manage all content filters from within one subsection of the `policyconfig` command. For that reason, adding the `drop_large_attachments` has been omitted from this example.

Table 3-127illustrates how to enable DLP policies on the default outgoing policy.

Code Example 3-128 DLP Policies for Default Outgoing Policy

```
mail3.example.com> policyconfig

Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 2


Outgoing Mail Policy Configuration
Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:     DLP:
-----           ---------- ------------------------------------------------
DEFAULT         Off            Off         Off             Off      Off
```

Code Example 3-128 DLP Policies for Default Outgoing 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
[]> edit

   Name:           Anti-Spam:     Anti-Virus: Content Filter: VOF:     DLP:
 -----           ---------- ----------------------------------------------

1. DEFAULT         Off            Off         Off             Off      Off

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

Policy Summaries:

Anti-Spam: Off
Anti-Virus: Off
Content Filters: Off (No content filters have been created)
Virus Outbreak Filters: Off
DLP: Off

Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- VOF - Modify Virus Outbreak Filters policy
- DLP - Modify DLP policy
[]> dlp


Choose the operation you want to perform:
- ENABLE - Enable DLP policy
[]> enable

1.        California AB-1298
2.        Suspicious Transmission - Zip Files
3.        Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[]> 1

1. Active California AB-1298
2.        Suspicious Transmission - Zip Files
3.        Restricted Files
```

Code Example 3-128 DLP Policies for Default Outgoing Policy

```
Enter the policy to toggle on/off, or press enter to finish:
[]> 2

1. Active California AB-1298
2. Active Suspicious Transmission - Zip Files
3.        Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[]> 3

1. Active California AB-1298
2. Active Suspicious Transmission - Zip Files
3. Active Restricted Files
Enter the policy to toggle on/off, or press enter to finish:
[]>

Policy Summaries:

Anti-Spam: Off
Anti-Virus: Off
Content Filters: Off (No content filters have been created)
Virus 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
- VOF - Modify Virus Outbreak Filters policy
- DLP - Modify DLP policy
[]>
```

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

Code Example 3-129 `quarantineconfig`

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

Code Example 3-129 `quarantineconfig` (Continued)

```
Currently configured quarantines:

 #  Quarantine Name    Size (MB)  % full  Messages  Retention  Policy
 1  Outbreak           3,072      0.0          1        12h    Release
 2  Policy             1,024      0.1        497        10d    Delete
 3  Virus              2,048      empty        0        30d    Delete

2,048 MB available for quarantine allocation.

Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- VOFMANAGE - Manage the Virus Outbreak Filters quarantine.
[]> new

Please enter the name for this quarantine:
[]> HRQuarantine

Please enter the maximum size for this quarantine in MB:
[]> 1024

Retention period for this quarantine. (Use 'd' for days or 'h' for hours.):
[]> 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" becomes full? [N]>

Do you want to give any users in the Operators/Guests
groups access to this quarantine?  [N]> y

No users in the Operators/Guests groups have access to "HRQuarantine"

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

    1.  hrquar
Select a user name or number
[]> 1
```

Code Example 3-129 `quarantineconfig` (Continued)

```
Users in the Operators/Guests groups with access to "HRQuarantine":
    1.  hrquar

Choose the operation you want to perform:

- DELETE - Delete a user.
[]>

Currently configured quarantines:

 #  Quarantine Name     Size (MB) % full  Messages  Retention  Policy
 1  HRQuarantine        1,024      N/A        N/A        15d   Release
 2  Outbreak            3,072      0.0          1        12h   Release
 3  Policy              1,024      0.1        497        10d   Delete
 4  Virus               2,048      empty        0        30d   Delete
(N/A: Quarantine contents is not available at this time.)

1,024 MB available for quarantine allocation.

Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- VOFMANAGE - Manage the Virus Outbreak Filters quarantine.
[]>
mail3.example.com> commit
```

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 scannned.
- Attachment scanning timeout is set at 180 seconds.
- Attachments that were not scanned are assumed to not match the search pattern. (This is the default behavior.)
- ASCII encoding is configured for use when none is specified for plain body text or anything with MIME type plain/text or plain/html.

Note — When setting the `assume the attachment matches the search pattern` to Y, messages that cannot be scanned will cause the message filter rule to evaluate to true. This could result in unexpected behavior, such as the quarantining of messages that do not match a dictionary, but were quarantined because their content could not be correctly scanned. This setting does not apply to RSA Email DLP scanning.

Code Example 3-130 `Scan Config` - Configuring Scan Behavior

```
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.
```

Code Example 3-130 `Scan Config` - Configuring Scan Behavior

```
- 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
[1]>

Configure encoding to use when none is specified for plain body text or
anything with MIME type plain/text or plain/html.
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
```

Code Example 3-130 `Scan Config` - Configuring Scan Behavior

```
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[1]> 1

Scan behavior changed.

There are currently 5 attachment type mappings configured to be
SKIPPED.

Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

[]> print
1. Fingerprint   Image
2. Fingerprint   Media
3. MIME Type     audio/*
4. MIME Type     image/*
5. MIME Type     video/*

>
```

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

Code Example 3-131 `stripheaders`

```
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.

Code Example 3-132 `textconfig` - Create Text Resources

```
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.
```

Code Example 3-132 `textconfig` - Create Text Resources

```
[]> new


What kind of text resource would you like to create?
1. Anti-Virus Container Template
2. Anti-Virus Notification Template
3. DLP Notification Template
4. Bounce and Encryption Failure Notification Template
5. Message Disclaimer
6. Encryption Notification Template (HTML)
7. Encryption Notification Template (text)
8. Notification Template
[1]> 5

Please create a name for the message disclaimer:
[]> disclaimer 1

Enter the encoding for the message disclaimer:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[1]>

Enter or paste the message disclaimer here.  Enter '.' on a blank line
to end.
This message was sent from an IronPort(tm) Email Security appliance.
.

Message disclaimer "disclaimer 1" created.


Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
```

Code Example 3-132 `textconfig` - Create Text Resources

```
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> delete

Please enter the name or number of the resource to delete:
[]> 1


Message disclaimer "disclaimer 1" has been deleted.


Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[]>
```

Use `textconfig -> EDIT` to modify an existing text resource. You can change the encoding or replace the text of the selected text resource.

Importing Text Resources

Use `textconfig -> IMPORT` to import a text file as a text resource. The text file must be present in the configuration directory on the appliance.

Code Example 3-133 `textconfig` - Importing a text file as a Text Resource

```
mail3.example.com> textconfig

Current Text Resources:
1. footer.2.message (Message Footer)

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> import

What kind of text resource would you like to create?
1. Anti-Virus Container Template
2. Anti-Virus Notification Template
3. DLP Notification Template
```

Code Example 3-133 `textconfig` - Importing a text file as a Text Resource (Continued)

```
4. Bounce and Encryption Failure Notification Template
5. Message Disclaimer
6. Encryption Notification Template (HTML)
7. Encryption Notification Template (text)
8. Notification Template
[1]> 8

Please create a name for the notification template:
[]> strip.mp3files

Enter the name of the file to import:
[]> strip.mp3.txt

Enter the encoding to use for the imported file:
1. US-ASCII
[ list of encodings ]
[1]>

Notification template "strip.mp3files" created.

Current Text Resources:
1. disclaimer.2.message (Message Disclaimer)
2. strip.mp3files (Notification Template)

Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>
```

Exporting Text Resources

Use `textconfig -> EXPORT` to export a text resource as a text file. The text file will be created in the configuration directory on the appliance.

Code Example 3-134 `textconfig` - Exporting a Text Resource as a Text File

```
mail3.example.com> textconfig

Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)
```

Code Example 3-134 `textconfig` - Exporting a Text Resource as a Text File (Continued)

```
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
- 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.

Creating a New Alert and Alert Recipient via the CLI

In this example, a new alert recipient (alertadmin@example.com) is created and set to receive critical system, hardware, and directory harvest attack alerts. The seconds to wait before sending a duplicate alert is set to 360 and the email From: address is set to Alerts@example.com.

Code Example 3-135 `alertconfig` - Creating a New Alert and Alert Recipient

```
mail3.example.com> alertconfig

Sending alerts to:
  joe@example.com
      Class: All - Severities: All

Seconds to wait before sending a duplicate alert (seconds): 300

Alerts will be sent using the system-default From Address.

IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
```

Code Example 3-135 `alertconfig` - Creating a New Alert and Alert Recipient (Continued)

```
- EDIT - Modify an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> 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. Virus Outbreak Filters
5. Anti-Virus
6. Anti-Spam
7. Directory Harvest Attack Prevention
[1]> 2,3,7
Select a Severity Level.  Separate multiple choices with commas.
1. All
2. Critical
3. Warning
4. Information
[1]> 2

Sending alerts to:
  joe@example.com
      Class: All - Severities: All
  alertadmin@example.com
      Class: Hardware - Severities: Critical
      Class: Directory Harvest Attack Prevention - Severities: Critical
      Class: System - Severities: Critical

Seconds to wait before sending a duplicate alert (seconds): 300

Alerts will be sent using the system-default From Address.

IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify an email address.
```

Code Example 3-135 `alertconfig` - Creating a New Alert and Alert Recipient (Continued)

```
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> setup

Seconds to wait before sending a duplicate alert (seconds):
[300]> 360

Would you like to enable IronPort AutoSupport, which automatically emails
system alerts and weekly status reports directly to IronPort Customer Care?
(Enabling AutoSupport is recommended.) [Y]>

Would you like to receive a copy of the weekly AutoSupport reports? [Y]>

Sending alerts to:
  joe@example.com
      Class: All - Severities: All
  alertadmin@example.com
      Class: Hardware - Severities: Critical
      Class: Directory Harvest Attack Prevention - Severities: Critical
      Class: System - Severities: Critical

Seconds to wait before sending a duplicate alert (seconds): 360

Alerts will be sent using the system-default From Address.

IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> from

Alerts will be sent using the system-default From Address.

Choose the operation you want to perform:
- EDIT - Edit the From Address.
[]> edit
```

Code Example 3-135 `alertconfig` - Creating a New Alert and Alert Recipient (Continued)

```
Please enter the From Address to use for alerts.
[]> Alerts@example.com

Sending alerts to:
  joe@example.com
      Class: All - Severities: All
  alertadmin@example.com
      Class: Hardware - Severities: Critical
      Class: Directory Harvest Attack Prevention - Severities: Critical
      Class: System - Severities: Critical

Seconds to wait before sending a duplicate alert (seconds): 360

Alerts will be sent using this configured From Address: Alerts@example.com

IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]>

mail3.example.com>
```

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 3-7 `grep` Command Options

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

Example of grep

The following example shows a search for the text string 'clean' or 'viral' within the antivirus logs. The grep command includes a regex expression:

Code Example 3-136 grep-Search for Text in a Log File

```
mail3.example.com> grep "CLEAN\\|VIRAL" antivirus

Fri Jun  9 21:50:25 2006 Info: sophos antivirus - MID 1 - Result 'CLEAN' ()
Fri Jun  9 21:53:15 2006 Info: sophos antivirus - MID 2 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 3 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 4 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 5 - Result 'CLEAN' ()
Fri Jun  9 22:47:41 2006 Info: sophos antivirus - MID 6 - Result 'CLEAN' ()
Fri Jun  9 22:47:42 2006 Info: sophos antivirus - MID 12 - Result 'CLEAN' ()
Fri Jun  9 22:53:04 2006 Info: sophos antivirus - MID 18 - Result 'VIRAL' ()
Fri Jun  9 22:53:05 2006 Info: sophos antivirus - MID 16 - Result 'VIRAL' ()
Fri Jun  9 22:53:06 2006 Info: sophos antivirus - MID 19 - Result 'VIRAL' ()
Fri Jun  9 22:53:07 2006 Info: sophos antivirus - MID 21 - Result 'VIRAL' ()
Fri Jun  9 22:53:08 2006 Info: sophos antivirus - MID 20 - Result 'VIRAL' ()
Fri Jun  9 22:53:08 2006 Info: sophos antivirus - MID 22 - Result 'VIRAL' ()
mail3.example.com>
```

logconfig

Description

Configure access to log files.

Usage

Commit: This command requires a 'commit'.

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

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

Example of FTP Push Log Subscription

In the following example, the `logconfig` command is used to configure a new delivery log called `myDeliveryLogs`. The log is then configured to be pushed via FTP to a remote host

Code Example 3-137 `logconfig` - Configuring a New Delivery Log

```
mail3.example.com> logconfig


Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP
Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
```

Code Example 3-137 `logconfig` - Configuring a New Delivery Log (Continued)

```
- 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
```

Code Example 3-137 `logconfig` - Configuring a New Delivery Log (Continued)

```
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
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP
Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "myDeliveryLogs" Type: "SMTP Conversation Logs" Retrieval: FTP Push -
Host
yourhost.example.com
```

Code Example 3-137 `logconfig` - Configuring a New Delivery Log (Continued)

```
16. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
17. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
18. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
19. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
20. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
21. "status" Type: "Status Logs" Retrieval: FTP Poll
22. "system_logs" Type: "System Logs" Retrieval: FTP Poll
23. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
24. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
```

Example of SCP Push Log Subscription

In the following example, the `logconfig` command is used to configure a new delivery log called `LogPush`. The log is configured to be pushed via SCP to a remote host with the IP address of 10.1.1.1, as the user `logger`, and stored in the directory `/tmp`. Note that the `sshconfig` command is automatically called from within the `logconfig` command when the log retrieval method is SCP push. (See "Configuring Host Keys" in the *IronPort AsyncOS Advanced User Guide* for information about Host keys, and "Managing Secure Shell (SSH) Keys" in the *IronPort AsyncOS User Guide* for more information about User keys.) Also note that an IP address can be used at the hostname prompt.

Code Example 3-138 `logconfig` - Creating a SCP 'Push' Delivery Log

```
mail3.example.com> logconfig

Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP
Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
```

Code Example 3-138 `logconfig` - Creating a SCP 'Push' Delivery Log (Continued)

```
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

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

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

Please enter the name for the log:
```

Code Example 3-138 `logconfig` - Creating a SCP 'Push' Delivery Log (Continued)

```
[]> LogPush

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


Hostname to deliver the logs:
[]> 10.1.1.1

Port to connect to on the remote host:
[22]>

Username on the remote host:
[]> logger

Directory on remote host to place logs:
[]> /tmp

Filename to use for log files:
[delivery.log]>

Maximum time to wait before transferring:
[3600]>

Maximum filesize before transferring:
[10485760]>

Protocol:
1. SSH1
2. SSH2
[2]> 2

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

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

Code Example 3-138 `logconfig` - Creating a SCP 'Push' Delivery Log (Continued)

```
SSH2:dsa
10.1.1.1 ssh-dss
AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwEsArt9LVE2ts5yE9JBTSdUwLvoq0G3FRqifrce9
2zgyHtc/
ZWyXavUTIM3Xd1bpiEcscMp2XKpSnPPx21y8bqkpJsSCQcM8zZMDjnOPm8ghiwHXYh7oNEUJCCPn
PxAy44rlJ5Yz4x9eIoALp0dHU0GR+j1NAAAAFQDQi5GY/
X9PlDM3fPMvEx7wc0edlwAAAIB9cgMTEFP1WTAGrlRtbowZP5zWZtVDTxLhdXzjlo4+bB4hBR7DK
uc80+naAFnThyH/J8R3WlJVF79M5geKJbXzuJGDK3Zwl3UYefPqBqXp2O1zLRQSJYx1WhwYz/
rooopN1BnF4sh12mtq3tde1176bQgtwaQA4wKO15k3zOWsPwAAAIAicRYat3y+Blv/
V6wdE6BBk+oULv3eK38gafuip4WMBxkG9GO6EQi8nss82oznwWBy/
pITRQfh4MBmlxTF4VEY00sARrlZtuUJC1QGQvCgh7Nd3YNais2CSbEKBEaIOTF6+SX2RNpcUF3Wg
5ygw92xtqQPKMcZeLtK2ZJRkhC+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 122606420764474441178474079962066753 25...3520565607
2. 10.1.1.1 ssh-dss AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwE...JRkhC+Vw==

Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display this machine's host keys.
[]>
Maximum filesize before transferring:
[10485760]>

Protocol:
1. SSH1
2. SSH2
[2]> 2

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

Currently installed host keys:

Choose the operation you want to perform:
- NEW - Add a new key.
- SCAN - Automatically download a host key.
- HOST - Display this machine's host keys.
[]> scan
```

Code Example 3-138 `logconfig` - Creating a SCP ‘Push’ Delivery Log (Continued)

```
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]> 4


SSH1:rsa
10.1.1.1 1024 35
122606420764474441178474079962066753259278682648965870690129496065430424463013457294798980627829828033793152226448694514316218272814453986931612508282328008815740072109975632356478532128816187806830746328234327778100131128176672666244511191783747965898000855947022484692079466697707373948871554575173520565607
```

Example of Syslog Push Log Subscription

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

Code Example 3-139 `logconfig` - Creating a SCP 'Push' Delivery Log

```
mail3.example.com> logconfig

Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP
Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

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

Code Example 3-139 `logconfig` - Creating a SCP 'Push' Delivery Log (Continued)

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

Please enter the name for the log:
[]> MailLogSyslogPush

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

Choose the method to retrieve the logs.
```

Code Example 3-139 `logconfig` - Creating a SCP 'Push' Delivery Log (Continued)

```
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> 4

Hostname to deliver the logs:
[]> 10.1.1.2

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

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

Currently configured logs:
1. "MailLogSyslogPush" Type: "IronPort Text Mail Logs" Retrieval: Syslog Push
-
Host 10.1.1.2
```

rollovernow

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

Code Example 3-140 `rollovernow`

```
mail3.example.com> rollovernow


Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP
Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
24. All Logs
Which log would you like to roll over?
[]> 2

Log files successfully rolled over.
mail3.example.com>
```

snmpconfig

Description

Configure SNMP.

Usage

Commit: This command requires a 'commit'.

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

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

Example

In the following example, the `snmpconfig` command is used to enable SNMP on the "PublicNet" interface on port 161. A passphrase for version 3 is entered and then re-entered for confirmation. The system is configured to service version 1 and 2 requests, and the community string `public` is entered for GET requests from those versions 1 and 2. The trap target of `snmp-monitor.example.com` is entered. Finally, system location and contact information is entered.

Code Example 3-141 `snmpconfig`

```
mail3.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

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

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

Please choose an IP interface for SNMP requests.
1. Data 1 (192.168.1.1/24: buttercup.run)
2. Data 2 (192.168.2.1/24: buttercup.run)
3. Management (192.168.44.44/24: buttercup.run)
[1]>

Enter the SNMPv3 passphrase.
>
Please enter the SNMPv3 passphrase again to confirm.
>
Which port shall the SNMP daemon listen on?
[161]>

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

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

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

Enter the Trap target (IP address). Enter "None" to disable traps.
```

Code Example 3-141 `snmpconfig` (Continued)

```
[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
```

Code Example 3-141 `snmpconfig` (Continued)

```
Location: Network Operations Center - west; rack #31, position 2
System Contact: Joe Administrator, x8888

mail3.example.com>
```

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

Code Example 3-142 `tail`

```
mail3.example.com> tail

Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP
Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
```

Code Example 3-142 `tail` (Continued)

```
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 19

Press Ctrl-C to stop.
Sat May 15 12:25:10 2008 Info: PID 274: User system commit changes: Automated
Update for Quarantine Delivery Host
Sat May 15 23:18:10 2008 Info: PID 19626: User admin commit changes:
Sat May 15 23:18:10 2008 Info: PID 274: User system commit changes: Updated
filter logs config
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Receiving
suspended.
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Suspended
receiving.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving
resumed.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving
resumed.
Sat May 15 23:48:17 2008 Info: PID 25696: User admin commit changes:
Sun May 16 00:00:00 2008 Info: Generated report: name b, start time Sun May 16
00:00:00 2004, size 2154 bytes
^Cmail3.example.com>
```

REPORTING

This section contains the following CLI commands:

- reportingconfig

reportingconfig

Using the `reportingconfig` command

The following subcommands are available within the reportingconfig submenu:

Table 3-8 `reportingconfig` Subcommands

Syntax	Description	Availability
`filters`	Configure filters for the Security Management appliance.	M-Series only
`alert_timeout`	Configure when you will be alerted due to failing to get reporting data.	M-Series only
`domain`	Configure domain report settings.	M-Series only
`mode`	Enable centralized reporting on the Security Management appliance. Enable centralized or local reporting for the Email Security appliance.	C-, M-Series
`mailsetup`	Configure reporting for the Email Security applaince.	C-Series only

Usage

Commit: This command requires a 'commit'.

Example: Enabling Reporting Filters (M-Series only)

Code Example 3-143 `reportingconfig` - Enabling reporting filters

```
mail3.example.com> reportingconfig


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing
to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> filters

Filters remove specific sets of centralized reporting data from the
"last year" reports.  Data from the reporting groups selected below
will not be recorded.

All filtering has been disabled.

1. No Filtering enabled
2. IP Connection Level Detail.
3. User Detail.
4. Mail Traffic Detail.
Choose which groups to filter, you can specify multiple filters by
entering a comma separated list:
[]> 2, 3


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing
to get
reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

Enabling HAT REJECT Information for Domain Reports (M-Series only)

Code Example 3-144 `reportingconfig` - Enabling HAT REJECT information for domain reports

```
mail3.example.com> reportingconfig


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
```

Code Example 3-144 `reportingconfig` - Enabling HAT REJECT information for domain reports

```
- ALERT_TIMEOUT - Configure when you will be alerted due to failing
to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> domain

If you have configured HAT REJECT policy on all remote appliances
providing reporting data to this appliance to occur at the message
recipient level then of domain reports.
Use message recipient HAT REJECT information for domain reports?
[N]> y


Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing
to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

Enabling Timeout Alerts (M-Series only)

Code Example 3-145 `reportingconfig` - Enabling timeout alerts

```
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

Code Example 3-146 `reportingconfig` - Enabling centralized reporting

```
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:
```

Code Example 3-146 `reportingconfig` - Enabling centralized reporting

```
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]>
```

Configure Storage Limit for Reporting Data (C-Series only)

Code Example 3-147 `reportingconfig` - Configure storage limit for centralized reporting data

```
esa01-vmw1-tpub.qa> 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
```

Code Example 3-147 `reportingconfig` - Configure storage limit for centralized reporting data

```
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

Code Example 3-148 `sbstatus` - Success

```
mail3.example.com> sbstatus

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

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

Code Example 3-149 `sbstatus` - Failure

```
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

Code Example 3-150 `senderbaseconfig`

```
ail3.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:

- listenerconfig
- localeconfig
- smtpauthconfig

listenerconfig

Description

The listenerconfig command allows you to create, edit, and delete a listener. IronPort 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 IronPort appliance communicates with the system that is injecting email.

Table 3-9 `listenerconfig` Commands

Name	Unique nickname you supply for the listener, for future reference. The names you define for listeners are case-sensitive. AsyncOS does not allow you to create two identical listener names.	
IP Interface	Listeners are assigned to IP interfaces. All IP interfaces must be configured using the `systemstartup` command or the `interfaceconfig` command before you create and assign a listener to it.	
Mail protocol	The mail protocol is used for email receiving: either ESMTP or QMQP	
IP Port	The specific IP port used for connections to the listener. by default SMTP uses port 25 and QMQP uses port 628.	

Table 3-9 `listenerconfig` Commands

Listener Type:	Public	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.
	Private	
	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 Chapter 9, "Testing and Troubleshooting" of the *AsyncOS Advanced User Guide* for more information.

Usage

Commit: This command requires a 'commit'.

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

Batch Command: This command supports a batch format.

Batch Format - General `listenerconfig`

The batch format of the `listenerconfig` command can be used to add and delete listeners on a particular interface. The batch format of the listenerconfig command also allows you to configure a listener's HAT and RAT.

- Adding a new listener:

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

- Deleting a listener:

```
listenerconfig delete <name>
```

Batch Format - HAT

The following examples demonstrate the use of the batch format of listenerconfig to perform various HAT-related tasks. For more information about arguments, consult Table 3-10, "`listenerconfig` Argument Values -HAT," on page 254

- 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 IronPort appliance

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

- Deleting all user defined sendergroups and policies from the HAT

```
listenerconfig edit <name> hostaccess clear
```

Table 3-10 `listenerconfig` Argument Values -HAT

Argument	Description
<behavior>	"Accept", "Relay", "Reject", "TCP Refuse", or "Continue". When selecting a behavior for use with a sendergroup, additional behaviors of the form "Policy: FOO" are available (where "FOO" is the name of policy).
<filename>	The filename to use with importing and exporting the hostaccess tables.
<group>	A sendergroup <name>.
<host>	A single entity of a <host_list>

Table 3-10 `listenerconfig` Argument Values -HAT

<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] NOTE: Separate multiple hosts with commas
<name>	The name of the sendergroup or policy. HAT labels must start with a letter or underscore, followed by any number of letters, numbers, underscores or hyphens.

Table 3-10 `listenerconfig` Argument Values -HAT

[options]	--max_size	Maximum message size. Add a trailing k for kilobytes, M for megabytes, or no letters for bytes.
	--max_conn	Maximum number of connections allowed from a single host.
	--max_msgs	Maximum number of messages per connection.
	--max_rcpt	Maximum number of recipients per message.
	--override	Override the hostname in the SMTP banner. “No” or SMTP banner string.
	--cust_acc	Specify a custom SMTP acceptance response. “No” or SMTP acceptance response string.
	--acc_code	Custom SMTP acceptance response code. Default is 220.
	--cust_rej	Specify a custom SMTP rejection response. “No” or SMTP rejection response string.
	--rej_code	Custom SMTP rejection response code. Default is 554.
	--rate_lim	Enable rate limiting per host. “No”, “default” or maximum number of recipients per hour per host.
	--cust_lim	Specify a custom SMTP limit exceeded response message. “No” or SMTP rejection response string. Default is “No”.
	--lim_code	Custom SMTP limit exceeded response code. Default is 452.
	--use_sb	Use SenderBase for flow control by default. “Yes”, “No”, or “default”.
	--as_scan	Enable anti-spam scanning. “Yes”, “No”, “Default”.
	--av_scan	Enable anti-virus scanning. “Yes”, “No”, “Default”.
	--dhap	Directory Harvest Attack Prevention. “No”, “default”, or maximum number of invalid recipients per hour from a remote host.
	--tls	Not supported; use menuing system to configure TLS.
	--sig_bits	Number of bits of IP address to treat as significant. From 0 to 32, “No” or “default”.

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 3-11, "`listenerconfig` Argument Values - RAT," on page 257

- Adding a new recipient to the RAT

```
listenerconfig edit <name> rcptacess new <rat_addr> [options]
```

- Editing a recipient in the RAT

```
listenerconfig edit <name> rcptacess edit <rat_addr> [options]
```

- Deleting a recipient from the RAT

```
listenerconfig edit <name> rcptacess delete <rat_addr>
```

- Printing a copy of the RAT

```
listenerconfig edit <name> rcptacess print
```

- Importing a local RAT to your IronPort appliance

```
listenerconfig edit <name> rcptacess import <filename>
```

- Exporting a RAT

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

- Clearing the default access

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

Table 3-11 `listenerconfig` Argument Values - RAT

Argument	Description
<rat_addr>	Enter the hosts to add. Hosts can be formatted as follows: CIDR addresses (10.1.1.0/24) Hostname (crm.example.com) Partial Hostname (.example.com) Usernames (postmaster@) Full email addresses (joe@example.com, joe@[1.2.3.4] NOTE: Separate multiple hosts with commas

Table 3-11 `listenerconfig` Argument Values - RAT

<options>	--action	Action to apply to address(es). Either "Accept" or "Reject". Default is "Accept".
	--cust_resp	Specify a custom SMTP response. "No" or SMTP acceptance response string.
	--resp_code	Custom SMTP response code. Default is 250 for "Accept" actions, 550 for "Reject".
	--bypass_rc	Bypass receiving control. Default is "No".
	--bypass_la	Bypass LDAP Accept query. Either "Yes" or "No."

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.

Code Example 3-151 listenerconfig - Adding a listener

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> new

Please select the type of listener you want to create.
1. Private
2. Public
3. Blackhole
[2]> 1

Please create a name for this listener (Ex: "OutboundMail"):
[]> OutboundMail

Please choose an IP interface for this Listener.
```

Code Example 3-151 listenerconfig - Adding a listener (Continued)

```
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
```

Code Example 3-151 listenerconfig - Adding a listener (Continued)

```
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
```

Example - 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 *IronPort AsyncOS User Guide*.

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

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`

Code Example 3-152 `listenerconfig` - Exporting the HAT

```
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
```

Code Example 3-152 `listenerconfig` - Exporting the HAT

```
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
=================
```

Code Example 3-152 `listenerconfig` - Exporting the HAT

```
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
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces:  No

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

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

$BLOCKED
    REJECT {}
$TRUSTED
    ACCEPT {
        tls = "off"
        dhap_limit = 0
        max_rcpts_per_hour = -1
        virus_check = "on"
        max_msgs_per_session = 5000
        spam_check = "off"
```

Code Example 3-152 `listenerconfig` - Exporting the HAT

```
        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
```

Code Example 3-152 `listenerconfig` - Exporting the HAT

```
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".
```

2. Outside of the Command Line Interface (CLI), get the file `inbound.HAT.txt`.
3. With a text editor, create new HAT entries in the file.

   In this example, the following entries are added to the HAT above the `ALL` entry:

```
spamdomain.com    REJECT
.spamdomain.com   REJECT
251.192.1.        TCPREFUSE
169.254.10.10     RELAY
```

   - The first two entries reject all connections from the remote hosts in the domain `spamdomain.com` and any subdomain of `spamdomain.com`.
   - 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 IronPort 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 *IronPort AsyncOS User Guide*.

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.)

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.

Code Example 3-153 `listnerconfig` - Importing the HAT

```
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
```

Code Example 3-153 `listnerconfig` - Importing the HAT (Continued)

```
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:
```

Code Example 3-153 `listnerconfig` - Importing the HAT (Continued)

```
[]> 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
```

Code Example 3-153 `listnerconfig` - Importing the HAT (Continued)

```
        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
```

Code Example 3-153 `listnerconfig` - Importing the HAT (Continued)

```
    $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 - Advanced HAT Parameters

Table 3-12 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 3-12

Table 3-12 Advanced HAT Parameter Syntax

Parameter	Syntax	Values	Example Values
Maximum messages per connection	`max_msgs_per_session`	Number	`1000`
Maximum recipients per message	`max_rcpts_per_msg`	Number	`10000` `1k`
Maximum message size	`max_message_size`	Number	`1048576` `20M`
Maximum concurrent connections allowed to this listener	`max_concurrency`	Number	`1000`
SMTP Banner Code	`smtp_banner_code`	Number	`220`
SMTP Banner Text (*)	`smtp_banner_text`	String	`Accepted`
SMTP Reject Banner Code	`smtp_banner_code`	Number	`550`
SMTP Reject Banner Text (*)	`smtp_banner_text`	String	`Rejected`
Override SMTP Banner Hostname	`use_override_hostname`	`on | off | default`	`default`
	`override_hostname`	String	`newhostname`
Use TLS	`tls`	`on | off | required`	`on`
Use anti-spam scanning	`spam_check`	`on | off`	`off`
Use Sophos virus scanning	`virus_check`	`on | off`	`off`
Maximum Recipients per Hour	`max_rcpts_per_hour`	Number	`5k`
Maximum Recipients per Hour Error Code	`max_rcpts_per_hour_code`	Number	`452`
Maximum Recipients per Hour Text (*)	`max_rcpts_per_hour_text`	String	`Too many recipients`
Use SenderBase	`use_sb`	`on | off`	`on`
Define SenderBase Reputation Score	`sbrs[`*value1*`:`*value2*`]`	`-10.0- 10.0`	`sbrs[-10:-7.5]`

Table 3-12 Advanced HAT Parameter Syntax

Parameter	Syntax	Values	Example Values
Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour	`dhap_limit`	Number	`150`

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.

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 3-13 SPF Control Settings

Conformance Level	Available SPF Control Settings
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)

Table 3-13 SPF Control Settings

Conformance Level	Available SPF Control Settings
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)

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.

Code Example 3-154 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
```

Code Example 3-154 SPF/SIDF Settings

```
Would you like to change SMTP actions taken for the HELO identity? [N]> y

What SMTP action should be taken if HELO check returns None?
1. Accept
2. Reject
[1]> 1

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

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

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

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

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

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

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

Verification timeout (seconds)
[40]>
```

The following shows how the SPF/SIDF settings are displayed for the listener's Default Policy Parameters.

Code Example 3-155 SPF/SIDF in Default Policy Parameters

```
SPF/SIDF Verification Enabled: Yes
  Conformance Level: SPF only
```

Code Example 3-155 SPF/SIDF in Default Policy Parameters

```
  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
```

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

Code Example 3-156 `localeconfig`

```
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:"

Code Example 3-157 `smtpauthconfig`

```
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]>
```

Code Example 3-157 `smtpauthconfig` (Continued)

```
Use SASL LOGIN mechanism when contacting forwarding server? [Y]>

Would you like to enter another forwarding server to this group? [N]>

Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
- EDIT - Edit an existing SMTP Auth profile
- PRINT - List all profiles
- DELETE - Delete a profile
- CLEAR - Delete all profiles
[]>

mail3.example.com> commit

Please enter some comments describing your changes:
[]> created SMTP auth profile

Changes committed: Tue Dec 21 12:51:56 2004 PST
```

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 IronPort C-Series 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

Code Example 3-158 systemsetup

```
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
```

Code Example 3-158 systemsetup

```
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
"0xffffff00"):
[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]>
```

Code Example 3-158 systemsetup

```
You have successfully configured the DNS settings.

*****

You are now going to configure how the IronPort C100 accepts mail by
creating a
"Listener".
Please create a name for this listener (Ex: "MailInterface"):
[]> InboundMail

Please choose an IP interface for this Listener.
1. Data 1 (192.168.1.1/24: ironport-C100.example.com)
[1]> 1

Enter the domain names or specific email addresses you want to accept
mail for.

Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are
allowed.
Separate multiple addresses with commas.
[]> example.com, .example.com

Would you like to configure SMTP routes for example.com, .example.com?
[Y]> n

Please specify the systems allowed to relay email through the IronPort
C100.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[]> example.com, .example.com

Do you want to enable filtering based on SenderBase Reputation Service
(SBRS)
Scores for this listener? (Your selection will be used to filter all
incoming
mail based on its SBRS Score.) [Y]> y

Do you want to enable rate limiting for this listener? (Rate limiting
defines
```

Code Example 3-158 systemsetup

```
the maximum number of recipients per hour you are willing to receive
from a
remote domain.) [Y]> y

Enter the maximum number of recipients per hour to accept from a
remote domain.
[]> 1000

Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: 1,000
Maximum Recipients Per Hour SMTP Response:
    452 Too many recipients received this hour
Use SenderBase for Flow Control:  Yes
Spam Detection Enabled:  Yes
Virus Detection Enabled:  Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
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
```

Code Example 3-158 systemsetup

```
IronPort Anti-Spam configured globally for the IronPort C100
appliance. Use the
policyconfig command (CLI) or Mail Policies (GUI) to customize the
IronPort
settings for each listener.

IronPort selected for DEFAULT policy

*****

Do you want to use Anti-Virus scanning in the default Incoming and
Outgoing
Mail policies? [Y]> y

1. McAfee Anti-Virus
2. Sophos Anti-Virus
Enter the number of the Anti-Virus engine you would like to use on the
default
Incoming and Outgoing Mail policies.
[]> 2

Sophos selected for DEFAULT policy

*****

Do you want to enable Virus Outbreak Filters? [Y]> y

Virus Outbreak Filters enabled.  The current threshold is 3.

Virus 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 Virus Outbreak Filters and
SenderBase.

*****

You will now configure system alerts.
Please enter the email address(es) to send alerts.
(Ex: "administrator@example.com")
```

Code Example 3-158 systemsetup

```
Separate multiple addresses with commas.
[]> administrator@example.com

Would you like to enable IronPort AutoSupport, which automatically
emails
system alerts and weekly status reports directly to IronPort Customer
Support?
You will receive a complete copy of each message sent to IronPort.
(Recommended) [Y]> y


*****

You will now configure scheduled reporting.
Please enter the email address(es) to deliver scheduled reports to.
(Leave blank to only archive reports on-box.)
Separate multiple addresses with commas.
[]> administrator@example.com


*****

You will now configure system time settings.
Please choose your continent:
1. Africa
2. America
...
11. GMT Offset
[11]> 2


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

Please choose your timezone:
1. Alaska Time (Anchorage)
...
26. Pacific Time (Los_Angeles)
```

Code Example 3-158 systemsetup

```
[]> 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.
```

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 does not support a batch format.

Example - Creating a New User Account

The following example shows how to create a new user account with a Help Desk User role..

Code Example 3-159 userconfig - Creating new user account

```
mail3.example.com> userconfig


Users:
1. admin - "Administrator" (admin)

External authentication: Disabled

Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- PASSWORD - Change the password for a user.
- EXTERNAL - Configure external authentication.
[]> new

Enter the new username.
[]> helpdesk1

Enter the full name for helpdesk1.
```

Code Example 3-159 userconfig - Creating new user account

```
[]> Help Desk

Assign a role to "helpdesk1":
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. Help Desk Users - Help Desk users have access only to ISQ and
Message Tracking.
[1]> 5

Enter the password for helpdesk1.
>
Please enter the new password again.
>

Users:
1. admin - "Administrator" (admin)
2. helpdesk1 - "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.
- PASSWORD - Change the password for a user.
- EXTERNAL - Configure external authentication.
[]>
```

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.

Code Example 3-160 userconfig - Setting up a RADIUS server

```
mail3.example.com> userconfig


Users:
1. admin - "Administrator" (admin)
```

Code Example 3-160 userconfig - Setting up a RADIUS server

```
External authentication: Disabled

Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- PASSWORD - Change the password for a user.
- EXTERNAL - Configure external authentication.
[]> external


Choose the operation you want to perform:
- SETUP - Set up global settings.
[]> setup

Do you want to enable external authentication? [N]> y

Please enter the timeout in seconds for how long the external
authentication credentials will be cached. (Enter '0' to disable
expiration of authentication credentials altogether when using one
time passwords.)
[0]> 30

Choose a mechanism to use:
LDAP is unavailable because no LDAP queries of type EXTERNALAUTH are
configured
1. RADIUS
[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.
```

Code Example 3-160 userconfig - Setting up a RADIUS server

```
>

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

1. CHAP
2. PAP
Select authentication type:
[2]> 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

Code Example 3-161 `password`

```
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 requires a 'commit'.

Cluster Management: This command is restricted to machine mode.

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

Example

Code Example 3-162 `last`

```
elroy.run> last

Username  Remote Host    Login Time        Logout Time       Total Time
========  =============  ================  ================  ==========
admin     10.251.23.186  Thu Sep 01 09:14  still logged in   1h 5m
admin     10.251.23.186  Wed Aug 31 14:00  Wed Aug 31 14:01  1m
admin     10.251.16.231  Wed Aug 31 13:36  Wed Aug 31 13:37  0m
admin     10.251.23.186  Wed Aug 31 13:34  Wed Aug 31 13:35  0m
admin     10.251.23.142  Wed Aug 31 11:26  Wed Aug 31 11:38  11m
admin     10.251.23.142  Wed Aug 31 11:05  Wed Aug 31 11:09  4m
admin     10.251.23.142  Wed Aug 31 10:52  Wed Aug 31 10:53  1m
admin     10.251.60.37   Tue Aug 30 01:45  Tue Aug 30 02:17  32m
admin     10.251.16.231  Mon Aug 29 10:29  Mon Aug 29 10:41  11m
shutdown                                   Thu Aug 25 22:20
```

who

Description

The `who` command lists all users who are logged into the system via the CLI, the time of login, the idle time, and the remote host from which the user is logged in.

Usage

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

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

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

Example

Code Example 3-163 `who`

```
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

Code Example 3-164 `whoami`

```
mail3.example.com> whoami

Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

VIRUS OUTBREAK FILTERS

This section contains the following CLI commands:

- vofconfig
- vofflush
- vofstatus
- vofstatus

vofconfig

Description

Use the `vofconfig` command to configure the Virus Outbreak Filters feature via the CLI. Configuration includes enabling the Virus Outbreak Filters feature, setting a threshold value, and selecting whether to receive email alerts for the Virus Outbreak Filters features.

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.

ExampleF

Code Example 3-165

```
mail3.example.com> vofconfig

VOF: enabled

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

Do you want to enable the Virus Outbreak Filters?  [Y]> y

Virus Outbreak Filters enabled.  The current threshold is 4.
Suspicious messages with a threat level that meet or exceed this
threshold will be quarantined.

Enter your threshold value.  This is a number between 1 and 5, where 1
is a very low tolerance for risk, and 5 is extremely high:
[4]> 2

Virus Outbreak Filters enabled.  The current threshold is 2.
```

Code Example 3-165 (Continued) (Continued)

```
Suspicious messages with a threat level that meet or exceed this
threshold will be quarantined.

VOF Alerts are sent when filetypes 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 VOF alerts?  [Y]> y

The Virus Outbreak Filters (VOF) 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 VOF for the desired
Incoming and Outgoing Mail Policies.


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

mail3.example.com> commit
```

vofflush

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

Code Example 3-166 `vofflush`

```
mail3.example.com> vofflush

Cached Outbreak Rules have been cleared.

mail3.example.com>
```

vofstatus

Description

The `vofstatus` command shows the current Virus Outbreak Filters feature settings, including whether the Virus 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

Code Example 3-167 `vofstatus`

```
mail3.example.com> vofstatus

   Virus Outbreak Filters: enabled

     Component              Last Update          Version
     Virus Outbreak Rules   Tue May 03 11:17:42  20050422_231148
     CASE - Core            Never                1.0.0-017
     CASE - Tools           Tue May 03 13:33:30  1.0.0-013

   Last download attempt made on Wed May 04 10:35:35

   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...

   Virus Outbreak Filter Rules with higher threat levels pose greater
   risks. (5 = highest threat, 1 = lowest threat)

   Last update: Tue May  3 11:17:46 2005

   Current Virus Outbreak Filters threshold: 3 (use "vofconfig" to change)

mail3.example.com>
```

vofupdate

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.

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

Example

Code Example 3-168 `vofupdate`

```
elroy.run> vofupdate

Requesting check for new CASE definitions
```