Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

April 27, 2010

CONTENTS

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide ■

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide ■

CHAPTER 7   **Other Tasks in the GUI**   **7-285**

CHAPTER 8   **Common Administrative Tasks**   **8-307**

CHAPTER **1**

Managing the IronPort Email Appliance

The *Cisco IronPort AsyncOS for Email Daily Management Guide* provides instructions for managing and monitoring the IronPort Email Security appliance on a regular basis. These instructions are designed for an experienced system administrator with knowledge of networking and email administration.

This chapter discusses the following topics:

The Email Security Appliance Documentation Set

The documentation for the 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.

Occasionally, this book refers to the other guides for additional information about topics. These guides are available on the Documentation CD that came with your IronPort appliance as well as the IronPort Customer Support Portal. For more information, see IronPort Nation, page 1-6.

How to Use This Guide

Use this guide as a resource to learn about how to manage and monitor your IronPort Email Security appliance on a regular basis. The topics are organized in a logical order. You might not need to read every chapter in the book. Review the Table of Contents and the section called How This Book Is Organized, page 1-3 to determine which chapters are relevant to your system.

You can also use this guide as a reference book. It contains important information, such as adding users and using support commands, that you can refer to throughout the life of the appliance.

The guide is distributed in print and electronically as PDF and HTML files. The electronic versions of the guide are available on the IronPort Customer Support Portal. You can also access the HTML online help version of the book directly from the appliance GUI by clicking the Help and Support link in the upper-right corner.

Before You Begin

Before you read this guide, review the *Cisco IronPort Quickstart Guide* and the latest product release notes for your appliance. In this guide, it is assumed that you have configured the IronPort C- or X-Series appliance for email delivery.

How This Book Is Organized

Chapter 1, "Managing the IronPort Email Appliance" provides an introduction to the Cisco IronPort appliance and defines its key features and role in the enterprise network.

Chapter 2, "Using Email Security Monitor" describes the Mail Flow Monitor feature: a powerful, web-based console that provides complete visibility into all inbound email traffic for your enterprise.

Chapter 3, "Tracking Email Messages" describes local message tracking. You can use message tracking to determine if a particular message was delivered, found to contain a virus, or placed in a spam quarantine.

Chapter 4, "Quarantines" describes the special queues or repositories used to hold and process messages. Messages in quarantines can be delivered or deleted, based on how you configured the quarantine. This includes the IronPort Spam quarantine.

Chapter 5, "Logging" describes the logging and log subscription functionality of the IronPort appliance.

Chapter 6, "Managing and Monitoring via the CLI" describes the commands available in the CLI available to you as you monitor the mail flow through the gateway.

Chapter 7, "Other Tasks in the GUI" describes typical administration tasks for managing and monitoring the Cisco IronPort appliance through the GUI.

Chapter 8, "Common Administrative Tasks" describes typical administration commands for managing and monitoring the Cisco IronPort appliance, such adding users, managing the configuration file, and managing SSH keys. This chapter also describes how to request technical support, allow IronPort customer support remote access to your IronPort, and use feature keys.

Chapter 9, "Testing and Troubleshooting" describes the process of creating so-called *black hole listeners* for testing the system performance and troubleshooting configuration problems.

Appendix A, "Accessing the Appliance" describes how to access the Cisco IronPort appliance for uploading and downloading files.

Typographic Conventions

Typeface	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 Cisco IronPort appliance.
`AaBbCc123`	User input, in contrast to on-screen computer output.	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**

AaBbCc123	Book titles, new terms, emphasized words, and command line variables; for command line variables, the italicized text is a placeholder for the actual name or value.	Read the *Cisco IronPort Quickstart Guide*.
		
		The Cisco 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`

Where to Find More Information

IronPort offers the following resources to learn more about the Email Security appliance.

Knowledge Base

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

```
http://www.ironport.com/support/login.html
```

Note You need a Support Portal account to access the site. If you do not already have an account, click the Request an Account link on the Support Portal login page. Generally, only IronPort customers, partners, and employees can access the Support Portal.

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.

IronPort Nation

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

You access IronPort Nation on the Customer Support Portal at the following URL:

```
http://www.ironport.com/support/login.html
```

IronPort Customer Support

You can request 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-IRON (4766)

International: `http://www.ironport.com/support/contact_support.html`

Support Portal: `http://www.ironport.com/support/login.html`

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

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-22160-02.

Using Email Security Monitor

The Email Security Monitor feature on the Cisco IronPort appliance is a powerful, web-based console that provides complete visibility into all inbound email traffic for your enterprise.

The Email Security Monitor feature integrates tightly into the system, collecting data from every step in the email delivery process, including reputation filtering, anti-spam, anti-virus scanning, Virus Outbreak Filters, policy enforcement (including content filters and data loss prevention), and message delivery. The database identifies and records each email sender by IP address, while interfacing with the SenderBase Reputation Service for real-time identity information. You can instantly report on any email sender's local mail flow history and show a profile that includes the sender's global record on the Internet. The Email Security Monitor feature allows your security team to "close the loop" on who is sending mail to your users, the amount of mail sent from and received by your users, and the effectiveness of your security policies.

This chapter explains how to:

- Access the Email Security Monitor feature to monitor inbound and outbound message flow.

- Make mail flow policy decisions (update whitelists, blacklists, and greylists) by querying for a sender's SenderBase Reputation Score (SBRS). You can query on network owners, domains, and even individual IP addresses.

- Report on mail flow, system status, and mail sent to and from your network.

This chapter contains the following sections:

Email Security Monitor Overview

For any given email sender for incoming mail, the Email Security Monitor database captures critical parameters such as:

• Message volume

• Connection history

• Accepted vs. rejected connections

• Acceptance rates and throttle limits

• Reputation filter matches

• Number of anti-spam messages for suspected spam and positively identified spam

• Number of virus-positive message detected by anti-virus scanning

See the "Anti-Spam" chapter in the *Cisco IronPort AsyncOS Configuration Guide* for more information on Anti-Spam scanning and the "Anti-Virus" chapter in the *Cisco IronPort AsyncOS Configuration Guide* for more information on anti-virus scanning.

The Email Security Monitor feature also captures information on which content filter a particular message triggers, including the internal user (email recipient) to or from which the message was sent.

The Email Security Monitor feature is available in the GUI only, and provides a view into your email traffic and the status of your IronPort appliance (including quarantines, work queues, and virus outbreaks). The appliance identifies when a sender falls outside of the normal traffic profile. Senders that do are highlighted in the interface, allowing you to take corrective action by assigning that sender to a sender group or refining the access profile of the sender; or, you can let AsyncOS's security services continue to react and respond. Outbound mail has a similar monitoring capability, providing you a view into the top domains in the mail queue and the status of receiving hosts (see Delivery Status Details Page, page 2-37).

Note   Information for messages present in the work queue when the appliance is
rebooted is not reported by the Email Security Monitor feature.

Email Security Monitor and Centralized Management

In this version of AsyncOS, you cannot aggregate Email Security Monitor reports
of clustered Cisco IronPort appliances. All reports are restricted to machine level.
This means they cannot be run at the group or cluster levels — only on individual
machines.

The same is true of the Archived Reports page — each machine in effect has its
own archive. Thus, the "Generate Report" feature runs on the selected machine.

The Scheduled Reports page is not restricted to machine level; therefore, settings
can be shared across multiple machines. Individual scheduled reports run at
machine level just like interactive reports, so if you configure your scheduled
reports at cluster level, every machine in the cluster will send its own report.

The "Preview This Report" button always runs against the login-host.

Email Security Monitor Pages

The Email Security Monitor feature is the first page displayed after you access the
GUI. To view the Email Security Monitor feature, access the GUI. (See the
"Overview" chapter in the *Cisco IronPort AsyncOS for Email Configuration
Guide*.) The Overview page on the Monitor menu is displayed. If you have
completed the System Setup Wizard (or the CLI `systemsetup` command) and
committed the changes, at least one public listener should already be configured
to accept email on your appliance. If the appliance is accepting email, the
Overview page will be populated with data.

The Email Security Monitor feature is comprised of all the pages available on the
Monitor menu except the Quarantines pages.

You use these pages in the GUI to monitor domains that are connecting to the
Cisco IronPort appliance's listeners. You can monitor, sort, analyze, and classify
the "mail flow" of your appliance and differentiate between high-volume senders
of legitimate mail and potential "spammers" (senders of high-volume, unsolicited

commercial email) or virus senders. These pages can also help you troubleshoot inbound connections to the system (including important information such as SBRS score and most recent sender group match for domains).

These pages help you classify mail relative to the appliance, and also relative to the services that exist beyond the scope of the gateway: the IronPort SenderBase Reputation Service, the IronPort Anti-Spam scanning service, the Anti-Virus scanning security services, content filters, and Virus Outbreak Filters.

You can generate a printer-friendly formatted .pdf version of any of the Email Security Monitor pages by clicking on the Printable PDF link at the top-right of the page. You can export graphs and other data to CSV (comma separated values) format via the **Export** link.

The exported CSV data will display all message tracking and reporting data in GMT regardless of what is set on the Email Security appliance. The purpose of the GMT time conversion is to allow data to be used independently from the appliance or when referencing data from appliances in multiple time zones.

Note If you export localized CSV data, the headings may not render properly in some browsers. This occurs because some browsers may not use the correct character set for the localized text. To work around this problem, you can save the file to disk, and open the file using File > Open. When you open the file, select the character set to display the localized text.

For more information about automating the export of report data, see Retrieving CSV Data, page 2-69).

Searching and Email Security Monitor

Many of the Email Security Monitor pages include a search form. You can search for four different types of items:

- IP Address
- domain
- network owner
- internal users
- destination domain

- internal sender domain

- internal sender IP address

- outgoing domain deliver status

For domain, network owner, and internal user searches, choose whether to exactly match the search text or look for items starting with the entered text (for instance, starts with "ex" will match "example.com").

For IP address searches, the entered text is always interpreted as the beginning of up to four IP octets in dotted decimal format. For instance, "17" will search in the range 17.0.0.0 through 17.255.255.255, so it will match 17.0.0.1 but not 172.0.0.1. For an exact match search, simply enter all four octets. IP address searches also support CIDR format (17.16.0.0/12).

All searches are bounded by the time range currently selected on the page.

The Overview Page

The Overview page provides a synopsis of the message activity of your IronPort appliance, including an overview of your quarantines and Virus Outbreak Filters status (in the System Overview section of the page). The Overview page also includes graphs and detailed message counts for incoming and outgoing messages. You can use this page to monitor the flow of all mail into and out of your gateway. The incoming and outgoing mail Summary Details show the number and percentage of messages categorized as clean, stopped by reputation filtering (SBRS), stopped as invalid recipient, spam detected, virus detected, stopped by content filter, and those considered "clean."

The Overview page highlights how the Cisco IronPort appliance is integrated with the IronPort SenderBase Reputation Service for incoming mail (messages stopped by reputation filtering, for example). On the **Overview** page, you can:

- View a mail trend graph of all mail "flowing" into or out of your gateway.

- View a graph showing the number of attempted messages, messages stopped by reputation filtering (SBRS), messages with invalid recipients, messages marked as spam, messages marked as virus positive, and clean messages, over time.

- View the summary of the system status and local quarantines.

- See current virus outbreak information based on information available at the IronPort Threat Operations Center (TOC).

The Overview page is divided into two sections: System Overview and Incoming and Outgoing Mail graphs and summary.

System Overview

The System Overview section of the Overview page serves as a system dashboard, providing details about the appliance including system and work queue status, quarantine status, and virus outbreak activity.

Figure 2-1   **System Overview Section of the Email Security Monitor Overview Page**

System Overview		
Status	System Quarantines - Top 3 by Disk Usage	Virus Threat Level
System Status: Online Incoming Messages per hour: 14.2k Messages in Work Queue: 0	Quarantine % Full Messages Policy 99.9% 67.7k Virus 0.3% 225	**No Virus Outbreak In Last 24 Hours** Outbreak Quarantine 0.0% full 0 messages
System Status Details	Local Quarantines	Outbreak Details ⊡

Status

This section provides an overview of the current state of the appliance and inbound mail processing.

System Status: One of the following states:

- Online

- Resource Conservation

- Delivery Suspended

- Receiving Suspended

- Work Queue Paused

- Offline

See the Chapter 6, "Managing and Monitoring via the CLI" for more information.

Incoming Messages: The average rate of incoming mail per hour. This projection is based on the number of incoming messages for the last 15 minutes (so if you have received 4 messages in the last 15 minutes, the hourly rate would be 16).

Work Queue: The number of messages awaiting processing in the work queue.

Click the System Status Details link to navigate to the System Status page.

System Quarantines

This section displays information about the top three quarantines by disk usage on the appliance, including the name of the quarantine, how full the quarantine is (disk space), and the number of messages currently in the quarantine.

Click the Local Quarantines link to navigate to the Local Quarantines page.

Virus Threat Level

This section shows the Virus Outbreak status as reported by the IronPort Threat Operations Center (TOC). For example, Figure 2-1 shows that a virus outbreak has been identified in the last 24 hours. Also shown is the status of the Outbreak quarantine, including how full it is (disk space) and the number of messages in the quarantine. The Outbreak quarantine is only displayed if you have enabled the Virus Outbreak Filters feature on your appliance.

Note   In order for the Virus Threat Level indicator to function, you need to have port 80 open on your firewall to "downloads.ironport.com." Alternatively, if you have specified a local update server, the Virus Threat Level indicator will attempt to use that address. The Virus Threat Level indicator will also update correctly if you have configured a proxy for downloads via the Service Updates page. For more information, see the "System Administration" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Click the Outbreak Details link to view the external IronPort TOC web site. Note that in order for this link to work, your IronPort appliance must be able to access the Internet. Note that the Separate Window icon () indicates that a link will open

in a separate window when clicked. You may need to configure your browser's pop-up blocker settings to allow these windows.

Incoming and Outgoing Summary and Graph

The Incoming and Outgoing summary sections provide access to real-time activity of all mail activity on your system and is comprised of the Incoming and Outgoing Mail Graphs and Mail Summaries. You can select the time frame on which to report via the Time Range menu. You can select Hour, Day, Week, or Month. The time range you select is used throughout all of the Email Security Monitor pages. The explanations of each type or category of message are below (see Categorizing Email, page 2-17).

The mail trend graph (left side, Figure 2-2) shows the breakdown of incoming mail in real-time.

While the mail trend graph displays a visual representation of the mail flow, the summary table (right side, Figure 2-2) provides a numeric breakdown of the same information. The summary table includes the percentage and actual number of each type of message, including the total number of attempted, threat, and clean messages.

The outgoing graph and summary show similar information for outbound mail.

Notes on Counting Messages in Email Security Monitor

The method Email Security Monitor uses to count incoming mail depends on the number of recipients per message. For example, an incoming message from example.com sent to three recipients would count as three messages coming from that sender.

Because messages blocked by reputation filtering do not actually enter the work queue, the appliance does not have access to the list of recipients for an incoming message. In this case, a multiplier is used to estimate the number of recipients. This multiplier was determined by IronPort Systems, Inc. and based upon research of a large sampling of existing customer data.

Figure 2-2   The Incoming Mail Graph and Summary Table
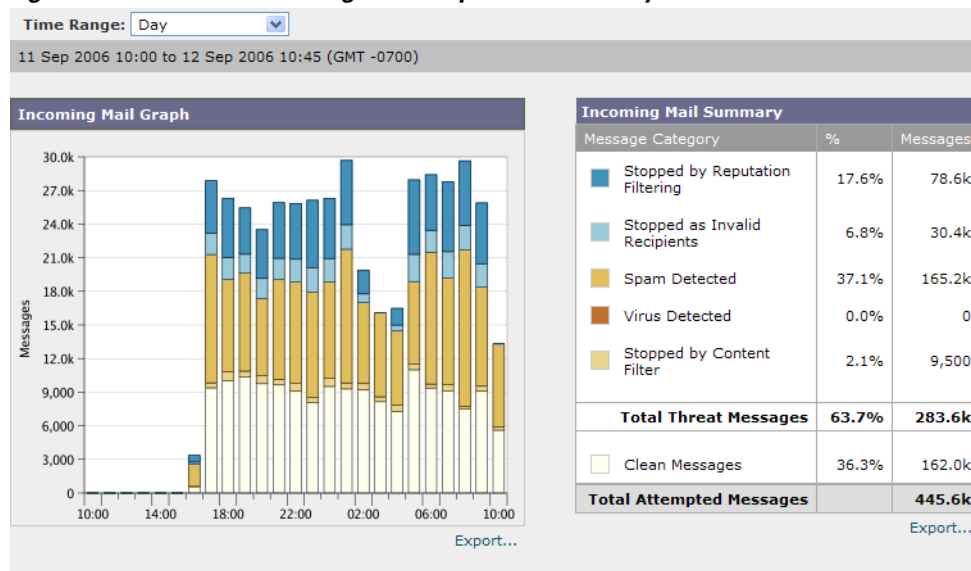
Categorizing Email

Messages reported in the Overview and Incoming Mail pages are categorized as follows:

Stopped by Reputation Filtering: All connections blocked by HAT policies multiplied by a fixed multiplier (see Notes on Counting Messages in Email Security Monitor, page 2-16) plus all recipients blocked by recipient throttling.

Invalid Recipients: All recipients rejected by conversational LDAP rejection plus all RAT rejections.

Spam Messages Detected: The total count of messages detected by the anti-spam scanning engine as positive or suspect and also those that were both spam and virus positive.

Virus Messages Detected: The total count and percentage of messages detected as virus positive and not also spam.

Note If you have configured your anti-virus settings to deliver unscannable or encrypted messages, these messages will be counted as clean messages and not virus positive. Otherwise, the messages are counted as virus positive.

Stopped by Content Filter: The total count of messages that were stopped by a content filter.

Clean Messages Accepted: Mail that is accepted and is deemed to be virus and spam free — the most accurate representation of clean messages accepted when taking per-recipient scanning actions (such as splintered messages being processed by separate mail policies) into account. However, because messages that are marked as spam or virus positive and still delivered are not counted, the actual number of messages delivered may differ from the clean message count.

Note Messages that match a *message* filter and are not dropped or bounced by the filter are treated as clean. Messages dropped or bounced by a message filter are not counted in the totals.

How Messages are Categorized

As messages proceed through the email pipeline, they can apply to multiple categories. For example, a message can be marked as spam or virus positive, it can also match a content filter. The various verdicts follow these rules of precedence: Virus Outbreak Filters quarantining (in this case the message is not counted until it is released from the quarantine and again processed through the work queue), followed by spam positive, virus positive, and matching a content filter.

For example, if a message is marked as spam positive, and your anti-spam settings are set to drop spam positive messages, the message is dropped and the spam counter is incremented. Further, if your anti-spam settings are set to let the spam positive message continue on in the pipeline, and a subsequent content filter drops, bounces, or quarantines the message, the spam count is still incremented. The content filter count is only incremented if the message is not spam or virus positive.

Incoming Mail Page

The **Incoming Mail** page provides a mechanism to report on the real-time information being collected by the Email Security Monitor feature for all remote hosts connecting to your appliance. This allows you to gather more information about an IP address, domain, and organization (network owner) sending mail to you. You can perform a Sender Profile search on IP addresses, domains, or organizations that have sent mail to you.

The Incoming Mail page has three views: Domain, IP Address, and Network Owner and provides a snapshot of the remote hosts connecting to the system in the context of the selected view.

Figure 2-3   The Incoming Mail Views

Incoming Mail: Domains

[IP Addresses | **Domains** | Network Owners]

It displays a table (Incoming Mail Details) of the top domains (or IP addresses, or network owners, depending on the view) that have sent mail to all public listeners configured on the appliance. You can monitor the flow of all mail into your gateway. You can click on any domain/IP/network owner to drill down to access details about this sender on a Sender Profile page (this is an Incoming Mail page, specific to the domain/IP/network owner you clicked on).

The Incoming Mail page extends to include a group of pages (Incoming Mail, Sender Profiles, and the Sender Group Report). From the **Incoming Mail** pages, you can:

- Perform a search on IP addresses, domains, or organizations (network owners) that have sent mail to you.

- View the Sender Groups report to see connections via a specific sender group and mail flow policy actions. See Sender Groups Report, page 2-32 for more information.

- See detailed statistics on senders which have sent mail to you, including the number of attempted messages broken down by security service (reputation filtering, anti-spam, anti-virus, etc.).

- Sort by senders who have sent you a high volume of spam or virus email, as determined by anti-spam or anti-virus security services.

- Use the IronPort SenderBase Reputation service to drill down on and examine the relationship between specific IP addresses, domains, and organizations to obtain more information about a sender.

- Drill down on specific senders to obtain more information about a sender from the IronPort SenderBase Reputation Service, including a sender's SenderBase Reputation Score and which sender group the domain matched most recently. Add senders to sender groups.

- Drill down on a specific sender who sent a high volume of spam or virus email, as determined by the anti-spam or anti-virus security services.

- Once you have gathered information on a domain, you can add the IP address, domain, or organization to an existing sender group (if necessary) by clicking "Add to Sender Group" from a domain, IP address, or network owner profile page. See the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Incoming Mail

The Incoming Mail page provides access to real-time activity of all public listeners configured on your system and is comprised of two main sections: the mail trend graphs summarizing the top domains received (by total threat messages and by total clean messages) and the Incoming Mail Details listing.

Figure 2-4   Incoming Mail Charts: Total Threat and Total Clean Messages

Time Range: Day

05 Nov 2006 12:00 to 06 Nov 2006 12:40 (GMT -0800)

Top Senders by Total Threat Messages

Domain	Value
No Domain Information	92.2k
charter.com	20.8k
comcast.net	17.3k
rr.com	15.2k
wanadoo.fr	13.1k
blueyonder.co.uk	11.0k
proxad.net	10.7k
shawcable.net	10.7k
verizon.net	8,022
bellsouth.net	7,022

Messages (0, 40.0k, 80.0k, 120.0k, 160.0k)

Top Senders by Clean Messages

Domain	Value
No Domain Information	25.7k
charter.com	15.1k
rr.com	11.3k
wanadoo.fr	10.4k
proxad.net	7,694
blueyonder.co.uk	7,321
shawcable.net	7,021
bellsouth.net	5,511
comcast.net	5,132
hotmail.com	5,103

Messages (0, 10.0k, 20.0k, 30.0k, 40.0k)

Export...   Export...

Figure 2-5   Incoming Mail Details

Incoming Mail Details

Items Displayed 10

Summary | All

Sender	Messages							
Domain	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Clean
No Domain Information	171.1k	83.8k	10.5k	42.1k	486	425	137.4k	33.7k
charter.com	34.8k	5,905	2,204	14.3k	59	167	22.7k	12.2k
shawcable.net	23.3k	2,986	1,415	9,952	61	169	14.6k	8,678
rr.com	24.0k	4,487	1,519	9,523	94	100	15.7k	8,285
hotmail.com	17.4k	6	1,118	8,773	68	97	10.1k	7,378
comcast.net	31.9k	14.7k	2,031	8,409	107	79	25.4k	6,575
wanadoo.fr	17.4k	2,755	1,146	7,137	61	90	11.2k	6,177
proxad.net	14.5k	3,008	947	5,609	53	76	9,693	4,856
blueyonder.co.uk	14.4k	3,369	884	5,431	30	83	9,797	4,600
dsl-verizon.net	10.8k	1,840	664	4,451	126	47	7,128	3,700

Export...

See Incoming Mail Details Listing, page 2-22 for an explanation of the data included in the Incoming Mail Details listing.

Notes on Time Ranges in the Mail Trend Graph

The Email Security Monitor feature constantly records data about the mail flowing into your gateway. The data are updated every 60 seconds, but the display shown is delayed by 120 seconds behind the current system time. You can "zoom out" from the day view to the week, day, and month views of the same data. Because the data is monitored in real time, information is periodically updated and summarized in the database.

The Email Security Monitor feature defines specific time ranges shown in Table 2-1.

Table 2-1   Time Ranges Defined in the Email Security Monitor Feature

This time range selected in the GUI	...is defined as:
Hour	the last 60 minutes
Day	the last 24 hours + the last 60 minutes
Week	the last 7 days + the last day by hours
Month	the last 30 days + the last day by hours

Incoming Mail Details Listing

The top senders which have connected to public listeners of the appliance are listed in the External Domains Received listing table at the bottom of the Incoming Mail page, based on the view selected. Click the column headings to sort the data. See Categorizing Email, page 2-17 for an explanation of the various categories.

The system acquires and verifies the validity of the remote host's IP address (that is, the domain) by performing a *double DNS lookup*. For more information about double DNS lookups and sender verification, see the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

The Sender Detail listing has two views, Summary and All.

The *Summary* view shows the total number of attempted messages for each sender, and includes a breakdown by category (the same categories as the Incoming Mail Summary graph on the Overview page: number of clean messages, stopped by reputation filtering, invalid recipients, spam detected, virus detected, and stopped by content filter).

The value for Stopped by Reputation Filtering is calculated based on several factors:

- Number of "throttled" messages from this sender.

- Number of rejected or TCP refused connections (may be a partial count).

- A conservative multiplier for the number of messages per connection.

When the appliance is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval. In this situation, the value shown can be interpreted as a "floor"; in other words, at least this many messages were stopped.

Note The Stopped by Reputation Filtering total on the Overview page is always based on a complete count of all rejected connections. Only the per-sender connection counts are ever limited due to load.

The *All* view shows the connection information (Accepted, Rejected) for senders as well as the breakdown by category. An additional column, Stopped by Recipient Throttling, lists throttled recipients.

Sort the listing by clicking the column header links. The sorting order is retained when you switch between the summary and all views, regardless of whether or not the sorted column exists in both views. In other words, if you sort the summary listing by "Total Attempted" and then switch to the All view, the data will retain its sorting.

These additional columns of data are summarized in the *All* view of the Sender Details table:

Connections Rejected: All connections blocked by HAT policies. When the appliance is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval.

Connections Accepted: All connections accepted

Stopped by Recipient Throttling: This is a component of Stopped by Reputation Filtering. It represents the number of recipient messages stopped because any of the following HAT limits have been exceeded: maximum recipients per hour,

maximum recipients per message, or maximum messages per connection. This is summed with an estimate of the recipient messages associated with rejected or TCP refused connections to yield Stopped by Reputation Filtering.

Total Threat: Total number of threat messages (stopped by reputation, stopped as invalid recipient, spam, plus virus)

"No Domain Information"

Domains which have connected to the appliance and could not be verified with a double-DNS lookup are automatically grouped into the special domain "No Domain Information." You can control how these types of unverified hosts are managed via Sender Verification. See the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

You can select the number of senders to show in the listing via the Items Displayed menu.

Querying for More Information

For senders listed in the Email Security Monitor summary table, click the sender (or "No Domain Information" link) to drill down for more information on the particular sender. The results are displayed on a Sender Profile page which includes real-time information from the IronPort SenderBase Reputation Service. From the Sender Profile page, you can drill down for more information on specific IP addresses or network owners (see Reporting Pages Populated with Data: Sender Profile Pages, page 2-24).

You can also view another report, the Sender Groups report, by clicking the Sender Groups report link at the bottom of the Incoming Mail page. For more information about Sender Groups reports, see Sender Groups Report, page 2-32.

Reporting Pages Populated with Data: Sender Profile Pages

If you clicked a sender in the Incoming Mail Summary table listed in the Incoming Mail page, the resulting *Sender Profile page* is listed with data for the particular IP address, domain, or organization (network owner). Sender Profile pages show detailed information for the sender. You can access a Sender Profile page for any network owner, domain, or IP address by clicking on the specified item in the Incoming Mail or other Sender Profile pages. Network owners are entities that contain domains; domains are entities that contain IP addresses. For more

information on this relationship and how it relates to the SenderBase Reputation Service, see the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

The Sender Profile pages displayed for IP addresses, network owners, and domains vary slightly. For each, the page contains a graph and summary table for incoming mail from this sender. Below the graph is a table listing domains or IP addresses associated with the sender (the Sender Profile page for individual IP addresses does not contain the detailed listing) and a information section with the current SenderBase, sender group, and network information for the sender.

- Network Owner profile pages contain information for the network owner, as well as the domains and IP addresses associated with that network owner.

- Domain profile pages contain information for the domains and IP addresses associated with that domain.

- IP address profile pages contain information about the IP address only.

Figure 2-6   Domains Listing for Network Owner

Domain	Rejected	Accepted	Throttled	Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Clean
Example.com	0	2,789	1,896	1,952	12.1k	0	642	12.4k
example-org.com	0	1	0	1	9	0	4	85
Example-com.com	0	3	0	2	77	0	6	79
Example.net	0	6	2	5	32	0	4	68
example-parnerNew.com	0	4	0	4	35	0	6	61
No Domain Information	0	56	88	14	34	0	0	56
examplePartner.com	0	3	0	3	12	0	2	44
mail3.example.com	0	1	0	1	14	0	0	44
mail2.example.com	0	1	0	1	35	0	0	41
mail.example.com	0	1	0	1	11	0	2	37

Items displayed 10

Export...

Each sender profile page contains the following data in the Current Information table at the bottom of the page:

- The **Global** information from the SenderBase Reputation Service, including:

  – IP Address, Domain Name, and/or Network Owner

  – Network Owner Category (Network Owner Only)

  – CIDR Range (IP addresses only)

- – Daily Magnitude and Monthly Magnitude for the IP address, Domain, and/or Network Owner

- – Days since the first message was received from this sender

- – Last sender group and whether DNS verified (IP Address sender profile page only)

Daily magnitude is a measure of how many messages a domain has sent over the last 24 hours. Similar to the Richter scale used to measure earthquakes, SenderBase magnitude is a measure of message volume calculated using a log scale with a base of 10. The maximum theoretical value of the scale is set to 10, which equates to 100% of the world's email message volume (approximately 10 billion messages/day). Using the log scale, a one-point increase in magnitude equates to a 10x increase in actual volume.

Monthly magnitude is calculated using the same approach as daily magnitude, except the percentages are calculated based on the volume of email sent over the last 30 days.

- – Average Magnitude (IP addresses only)

- – Lifetime Volume / 30 Day Volume (IP address profile pages only)

- – Bonded Sender Status (IP address profile pages only)

- – SenderBase Reputation Score (IP address profile pages only)

- – Days Since First Message (network owner and domain profile pages only)

- – Number of Domains Associated with this Network Owner (network owner and domain profile pages only)

- – Number of IP Addresses in this Network Owner (network owner and domain profile pages only)

- – Number of IP Addresses used to Send Email (network owner pages only)

Click the "More from SenderBase" link to see a page with all information supplied by the SenderBase Reputation Service.

- • The **Mail Flow Statistics** information, with Email Security Monitor information collected about the sender over the last hour, day, week, month, and year.

- • **Details** about the domains and IP addresses controlled by this network owner are displayed on network owner profile pages. Details about the IP addresses in the domain are displayed on domain pages.

From a domain profile page, you can drill down to a specific IP address, or drill up to view an organization profile page.

If you are an administrator of the system, on each of these pages, you can choose to add the network owner, domain, or IP address to a sender group by clicking the check box for the entity (if necessary) and then clicking Add to Sender Group.

You can also add a sender to a sender group by clicking the **Add to Sender Group** link below the Sender Group Information in the Current Information table for the sender and clicking Add to Sender Group. For more information about adding senders to sender groups, see the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*. Of course, you do not have to make any changes — you can let the security services handle incoming mail.

Figure 2-7   Current Information for Network Owner

Current Information for EXAMPLE COM	
Current Information from SenderBase	Sender Group Information
Network Owner Category: NSP Daily Magnitude: 7.8 Monthly Magnitude: 7.5 Days Since First Message from this Network Owner: -- days Number of Domains Associated with this Network Owner: 1,928 Number of IP Addresses Used to Send Mail: 3.7M	Last Sender Group: UNKNOWNLIST
More from SenderBase 🗗	Add to Sender Group...

Sender Profile Search

Type an IP address, a domain, or an organization name in the Quick Search box to search for a specific sender.

A Sender Profile page is displayed with the information for sender. See Reporting Pages Populated with Data: Sender Profile Pages, page 2-24.

Figure 2-8   Domain Profile Page (1 of 2)

Sender Profile: rr.com

Printable (PDF)

| Time Range: | Day |

11 Sep 2006 14:00 to 12 Sep 2006 14:39 (GMT -0700)

Incoming Mail from this Domain

Messages by Category	%	Messages
Stopped by Reputation Filtering	7.7%	1,790
Invalid Recipients	6.5%	1,516
Spam Detected	54.0%	12.5k
Virus Detected	0.0%	0
Stopped by Content Filter	2.3%	540
Clean	29.4%	6,810
Total Attempted:	**100.0%**	**23.2k**

Export...

Connections by Category	%	Connections
Rejected	0.0%	0
Accepted	100.0%	2,310
Total Connections:	**100.0%**	**2,310**

Export...

Figure 2-9   Domain Profile Page (2 of 2)

IP Addresses

Items displayed 10 ▼

| Messages | Sender Information |

Sender		Messages					
IP Address	Hostname	Total Attempted	Stopped by Reputation	Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Clean
24.173.61.70	...0.sw.biz.rr.com	102	0	2	28	0	4	68
24.106.19.142	...west.biz.rr.com	84	0	2	21	0	2	59
65.32.5.134	...tampabay.rr.com	123	0	5	60	0	2	56
24.162.6.167	...ston.res.rr.com	88	0	2	27	0	4	55
24.105.129.12	....nyc.biz.rr.com	95	0	1	34	0	6	54
24.26.237.55	...satx.res.rr.com	102	0	0	54	0	2	46
24.167.87.7	...ston.res.rr.com	101	0	3	51	0	2	45
65.31.125.212	...2.wi.res.rr.com	129	0	3	75	0	6	45
24.30.203.204	mxb.biz.rr.com	73	0	1	24	0	4	44
24.123.207.90	...tral.biz.rr.com	98	0	2	52	0	0	44

Export...

Current Information for rr.com

Current Information from SenderBase	Sender Group Information	Network Information
Daily Magnitude: 8.1 Monthly Magnitude: 7.7 Days Since First Message from this Domain: 2521.1 days	Last Sender Group: ALL	Network Owner: Road Runner
More from SenderBase ⬏	Add to Sender Group...	

Figure 2-10   Network Owner Profile Page (1 of 2)

Sender Profile: Road Runner   Printable (PDF)

Time Range: Day

11 Sep 2006 14:00 to 12 Sep 2006 14:43 (GMT -0700)

Incoming Mail from this Network Owner

Messages by Category	%	Messages
Stopped by Reputation Filtering	8.3%	1,484
Invalid Recipients	6.4%	1,155
Spam Detected	55.8%	10.0k
Virus Detected	0.0%	0
Stopped by Content Filter	2.4%	438
Clean	27.1%	4,876
Total Attempted:	**100.0%**	**18.0k**

Export...

Connections by Category	%	Connections
Rejected	0.0%	0
Accepted	100.0%	1,820
Total Connections:	**100.0%**	**1,820**

Export...

Figure 2-11   Network Owner Profile Page (2 of 2)

Domain	Rejected	Accepted	Throttled	Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Clean
Domains								
rr.com	0	1,811	1,473	1,151	10.0k	0	438	4,868
mybrighthouse.com	0	3	0	3	18	0	0	6
No Domain Information	0	6	11	1	10	0	0	2

Export...

Current Information for Road Runner

Current Information from SenderBase	Sender Group Information
Network Owner Category: NSP Daily Magnitude: 8.2 Monthly Magnitude: 8.0 Days Since First Message from this Network Owner: -- days Number of Domains Associated with this Network Owner: 334 Number of IP Addresses Used to Send Mail: 5.7M	Last Sender Group: UNKNOWNLIST
More from SenderBase	Add to Sender Group...

Figure 2-12   IP Address Profile Page (1 of 2)

Sender Profile: 65.32.5.134   ms-smtp-04.tampabay.rr.com   Printable (PDF)

Time Range: Day

11 Sep 2006 14:00 to 12 Sep 2006 14:46 (GMT -0700)

Incoming Mail from this IP Address

Messages by Category	%	Messages
Stopped by Reputation Filtering	0.0%	0
Invalid Recipients	4.1%	5
Spam Detected	48.8%	60
Virus Detected	0.0%	0
Stopped by Content Filter	1.6%	2
Clean	45.5%	56
Total Attempted:		123

Export...
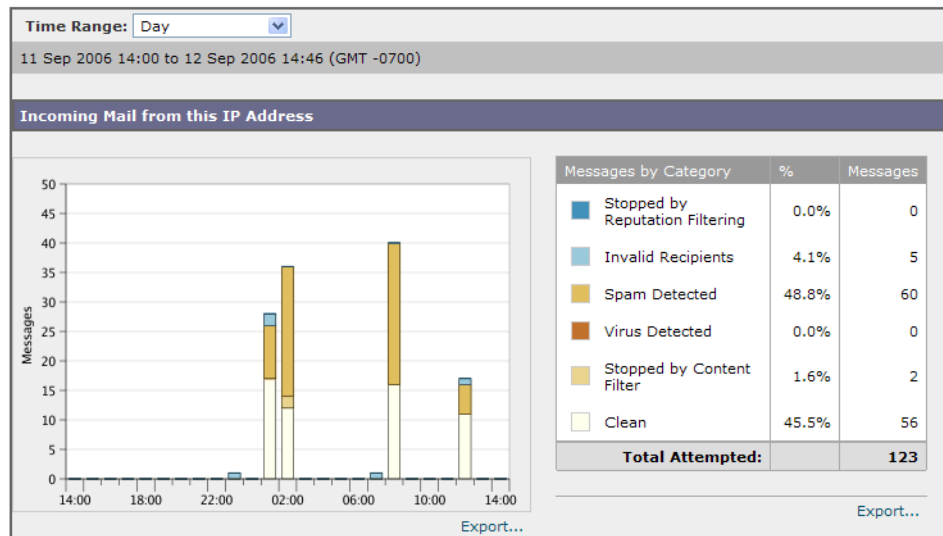
Figure 2-13   *IP Address Profile Page (2 of 2)*

Current Information for 65.32.5.134		
Current Information from SenderBase	Sender Group Information	Network Information
SenderBase Reputation Score (SBRS): 3 Bonded Sender Status: 0 Daily Magnitude: 5.1 Monthly Magnitude: 4.6 CIDR Range: 14 Average Magnitude: 5.8	Last Sender Group: ALL DNS Verified: Yes	Network Owner: Road Runner Domain: rr.com
More from SenderBase ⊡	Add to Sender Group...	

Sender Groups Report

The Sender Groups report provides a summary of connections by sender group and mail flow policy action, allowing you to review SMTP connection and mail flow policy trends. The Mail Flow by Sender Group listing shows the percentage and number of connections for each sender group. The Connections by Mail Flow Policy Action chart shows the percentage of connections for each mail flow policy action. This page provides an overview of the effectiveness of your Host Access Table (HAT) policies. For more information about the HAT, see the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Figure 2-14   *Sender Groups Report Page*
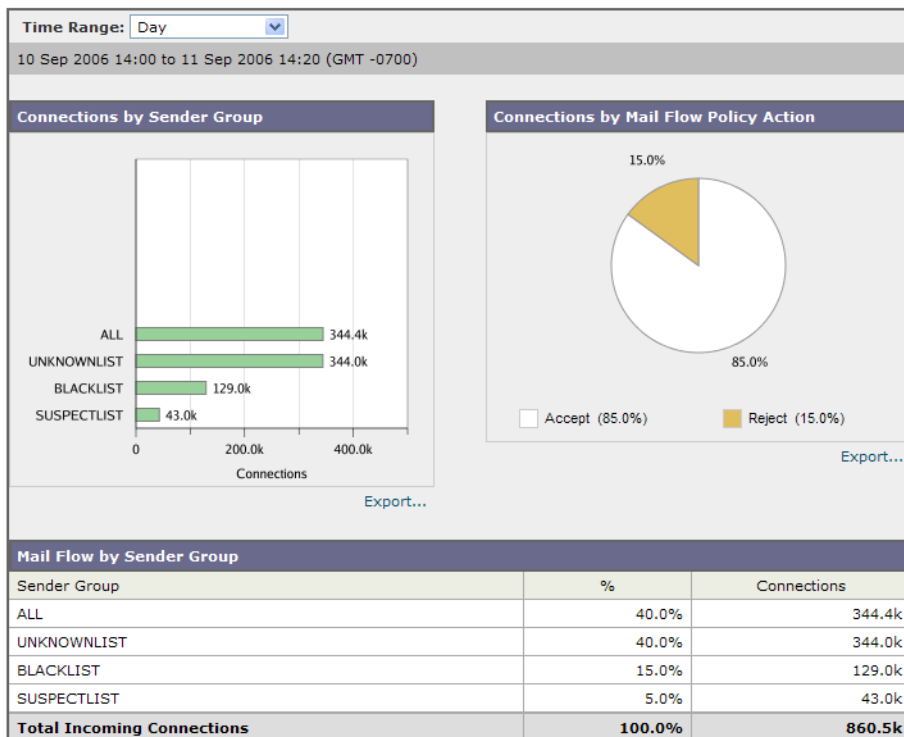
Outgoing Destinations

The Outgoing Destinations page provides information about the domains your company sends mail to. The page consists of two section. The top half of the page consists of graphs depicting the top destinations by outgoing threat messages and top destinations by outgoing clean messages on the top half of the page. The bottom half of the page displays a chart showing all the columns sorted by total recipients (default setting).

You can select a time range on which to report (hour, day, week, or month). As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

The Outgoing Destinations page can be used to answer the following types of questions:

- What domains is the IronPort appliance sending mail to?

- How much mail is sent to each domain?

- How much of that mail is clean, spam-positive, virus-positive, or stopped by a content filter?

- How many messages are delivered and how many messages are hard-bounced by the destination server?

Figure 2-15   Outgoing Destinations Page

Outgoing Destinations

Printable (PDF)

Time Range: Month (30 days) ▼

21 Jul 2007 00:00 to 20 Aug 2007 10:48 (GMT -0700)

Top Destinations by Total Threat Messages

qa12.qa   2,017
qa16.qa   462
blah.qa   11

0   1,000   2,000   3,000   4,000

Messages

Info... | Export...

Top Destinations by Clean Messages

qa12.qa   2.5M
qa16.qa   566.7k
blah.qa   7,526

0   1.0M   2.0M   3.0M   4.0M

Messages

Info... | Export...

Outgoing Destinations Detail

Destination	Messages						Delivery		
Domain	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Clean	Total Processed ▼	Hard Bounced	Delivered	Total Messages Delivered
qa12.qa	0	2,017	0	2,017	2.5M	2.5M	1.0M	1.2M	2.2M
qa16.qa	0	462	0	462	566.7k	567.1k	489.6k	0	489.6k
blah.qa	0	11	0	11	7,526	7,537	7,380	0	7,380

Info... | Export...

Outgoing Senders

The Outgoing Senders page provides information about the quantity and type of mail being sent from IP addresses and domains in your network. You can view the results by domain or IP address when you view this page. You might want to view

the results by domain if you want to see what volume of mail is being sent by each domain, or you might want to view the results by IP address if you want see which IP addresses are sending the most virus messages or triggering content filters.

The page consists of two sections. On the left side of the page is a graphs depicting the top senders by total threat messages. Total threat messages include messages that are spam or virus positive or triggered a content filter. On the right side of the page is a graph displaying top senders by clean messages on the top half of the page. The bottom half of the page displays a chart showing all the columns sorted by total messages (default setting).

Note   This page does not display information about message delivery. Delivery information, such as how many messages from a particular domain were bounced can be tracked using the Delivery Status page.

You can select a time range on which to report (hour, day, week, or month). As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

The Outgoing Senders page can be used to answer the following types of questions:

- Which IP addresses are sending the most virus or spam positive email?

- Which IP addresses trigger content filters the most frequently?

- Which domains are sending the most mail?

Figure 2-16   Outgoing Senders Page (IP Addresses Displayed)

Outgoing Senders: IP Addresses
[Domains | **IP Addresses**]
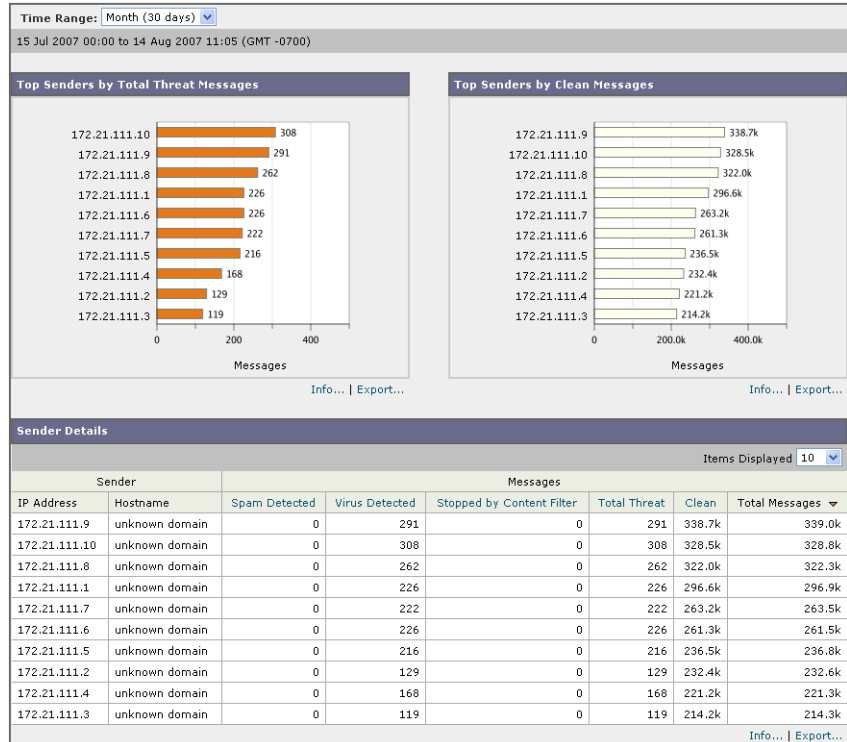
The Delivery Status Page

If you suspect delivery problems to a specific recipient domain or if you want to gather information on a Virtual Gateway address, the Monitor > Delivery Status Page provides monitoring information about email operations relating to a specific recipient domain.

The **Delivery Status Page** displays the same information as the `tophosts` command within the CLI. (For more information, see "Determining the Make-up of the Email Queue" in Chapter 6, "Managing and Monitoring via the CLI.")

This page displays a list of the top 20, 50, or 100 recipient domains for messages delivered by the system within the last three hours. You can sort by latest host status, active recipients (the default), connections out, delivered recipients, soft bounced events, and hard bounced recipients by clicking the links in the column heading for each statistic.

- To search for a specific domain, type the name of the domain in the Domain Name: field and click **Search**.

- To drill down on a domain shown, click the domain name link.

The results are shown in an Delivery Status Details Page.

Note Any activity for a recipient domain results in that domain being "active" and thus present in the overview page. For example, if mail remains in the outbound queue due to delivery problems, that recipient domain continues to be listed in the outgoing mail overview.

Retrying Delivery

Messages that are scheduled for later delivery can be immediately retried by clicking **Retry All Delivery**. Retry All Delivery allows you to reschedule messages in the queue for immediate delivery. All domains that are marked as "down" and any scheduled or soft bounced messages are queued for immediate delivery.

To retry delivery to a specific destination domain, click the domain name link. On the Delivery Status Details page, click **Retry Delivery**.

You can also use the `delivernow` command in the CLI to reschedule messages for immediate delivery. For more information, see Scheduling Email for Immediate Delivery, page 6-268.

Delivery Status Details Page

Use the **Delivery Status Details Page** to look up statistics on a specific recipient domain. This page displays the same information as the `hoststatus` command within the CLI: Mail Status, Counters and Gauges. (For more information, see "Monitoring the Status of a Mail Host" in Chapter 6, "Managing and Monitoring

via the CLI.") To search for a specific domain, type the name of the domain in the Domain Name: field and click **Search**. Virtual Gateway address information appears if you are using the `altsrchost` feature.

Figure 2-17   Delivery Status Page

Delivery Status

Printable (PDF)

Outgoing Destinations Status

Retry All Delivery

Destination Domain	Latest Host Status	Active Recipients ▼	Connections Out	Delivered Recipients	Soft Bounced	Hard Bounced
aol.com.d1.qa12.qa	Down	62.0k	0	0	0	86.6k
webtv.net.d1.qa16.qa	Down	8,654	0	0	0	16.1k
earthlink.net.d1.qa16.qa	Down	4,266	0	0	0	7,983
worldnet.att.net.d1.qa16.qa	Down	3,531	0	0	0	6,470
home.com.d1.qa16.qa	Down	3,195	0	0	0	6,141
excite.com.d1.qa16.qa	Down	2,847	0	0	0	5,347
mindspring.com.d1.qa16.qa	Down	2,655	0	0	0	5,094
msn.com.d1.qa16.qa	Down	2,638	0	0	0	5,053
bigfoot.com.d1.qa16.qa	Down	2,455	0	0	0	4,508
juno.com.d1.qa16.qa	Down	2,379	0	0	0	4,663

Info... | Export...

Search for: [Outgoing Domain Delivery Status ▼] [ ] [exact match ▼] [Search] ?

Figure 2-18   Delivery Status Details Page

Delivery Status Details: ironport.com

Printable (PDF)

Status Summary

Host Status		Delivery Information	
Host Up/Down:	Down	Last Activity:	19 Feb 2010 01:14 (GMT)
Status as of:	19 Feb 2010 01:15 (GMT)	Next Delivery:	N/A
Expiration Time for Ordered IP Addresses:	19 Feb 2010 01:30 (GMT)	Oldest Message:	15 mins 32 secs
		Last 5XX Error:	N/A
Virtual Gateways:	No Virtual Gateways defined	Last TLS Error:	N/A

Retry Delivery

Delivery Status Details

Ordered IP Addresses

		Rate Limiting		
Preference	IP Address	Recipients	Limit	Minutes Remaining
10	172.21.116.1	N/A	N/A	N/A

Counters		**Gauges**	
Queue		Queue	
Soft Bounced Events	0	Unattempted Recipients	2,675
Completion		Attempted Recipients	0
DNS Hard Bounces	0	**Active Recipients:**	**2,675**
5XX Hard Bounces	0	Connections	
Filter Hard Bounces	0	Current Outgoing Connections	0
Expired Hard Bounces	5,094	Pending Outgoing Connections	0
Other Hard Bounces	0	Throttle	
Hard Bounced Recipients:	**5,094**	Current Recipients	0
Delivered Recipients:	**0**	Recipient Limit	0
Deleted Recipients:	**0**	Minutes Remaining	60
Completed Recipients:	**5,094**		

The Internal Users Page

The Internal Users page provides information about the mail sent and received by your internal users, *per email address* (a single user may have multiple email addresses listed — the email addresses are not combined in the report).

The page consists of two sections: graphs depicting the top users by clean incoming and outgoing messages, and user mail flow details. You can select a time range on which to report (hour, day, week, or month). As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

The User Mail Flow Details listing breaks down the mail received and sent by each email address into Clean, Spam Detected (incoming only), Virus Detected, and Content Filter Matches. You can sort the listing by clicking on the column headers.

Using the Internal Users report, you can answer these kinds of questions:

- Who is sending the most external email?
- Who receives the most clean email?
- Who receives the most spam?
- Who is triggering which content filters?
- Whose email is getting caught by content filters?

Inbound Internal Users are the users for which you received email, based on the Rcpt To: address. Outbound Internal Users are based on the Mail From: address and are useful when tracking the types of email that senders on your internal network are sending.

Note that some outbound mail (like bounces) have a null sender. They are counted under outbound and "unknown."

Click on an internal user to view the Internal User detail page for that user.

Internal User Details

The Internal User detail page shows detailed information about the specified user, including a breakdown of incoming and outgoing messages showing the number of messages in each category (spam detected, virus detected, stopped by content filter, and clean). Incoming and outgoing content filter and DLP policy matches are also shown.

Figure 2-19   Internal User Details Page

Click on a content filter name to view detailed information for that filter in the corresponding content filter information page (see The Content Filters Page, page 2-45). You can use this method to get a list of users who also sent or received mail that matched that particular content filter.

Searching for a Specific Internal User

You can search for a specific internal user (email address) via the search form at the bottom of the Internal Users page and the Internal User detail page. Choose whether to exactly match the search text or look for items starting with the entered text (for instance, starts with "ex" will match "example.com").

Figure 2-20   Internal User Search Results

The DLP Incidents Page

The DLP Incidents page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The IronPort appliance uses the DLP email policies enabled in the Outgoing Mail Policies table to detect sensitive data sent by your users. Every occurrence of an outgoing message violating a DLP policy is reported as an incident.

Using the DLP Incidents report, you can answer these kinds of questions:

- What type of sensitive data is being sent by your users?

- How severe are these DLP incidents?

- How many of these messages are being delivered?

- How many of these messages are being dropped?

- Who is sending these messages?

The DLP Incidents page is comprised of two main sections:

- the DLP incident trend graphs summarizing the top DLP incidents by severity (Low, Medium, High, Critical) and policy matches, and

- the DLP Incidents Details listing.

You can select a time range on which to report (hour, day, week, or month). As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link or PDF format by clicking the **Printable (PDF)** link.

Figure 2-21   DLP Incidents Charts: Top Incidents by Severity, Incident Summary, and Top DLP Policy Matches
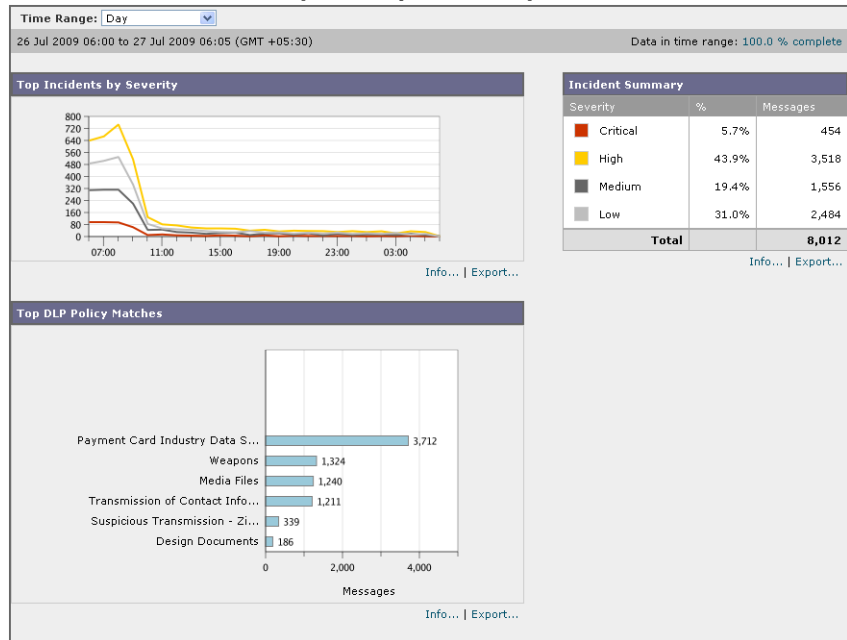
Figure 2-22   DLP Incident Details

Click on the name of a DLP policy to view detailed information on the DLP incidents detected by the policy. You can use this method to get a list of users who sent mail that contained sensitive data detected by the policy.

DLP Incidents Details

The DLP policies currently enabled in the appliance's outgoing mail policies are listed in the DLP Incidents Details table at the bottom of the DLP Incidents page. Click on the name of a DLP policy to view more detailed information.

The DLP Incidents Details table shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped. Click on the column headings to sort the data.

DLP Policy Detail Page

If you clicked the name of a DLP policy in the DLP Incidents Details table, the resulting DLP Policy Detail page displays the DLP incidents data for the policy. The page displays graphs on the DLP incidents based on severity.

The page also includes an Incidents by Sender listing at the bottom of the page that lists each internal user who has sent a message that violated the DLP policy. The listing also shows the total number of DLP incidents for this policy per user, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped. You can use the Incidents by Sender listing to find out which users may be sending your organization's sensitive data to people outside your network.

Figure 2-23   DLP Policy Details Charts: Top Incidents by Severity, Incident Summary
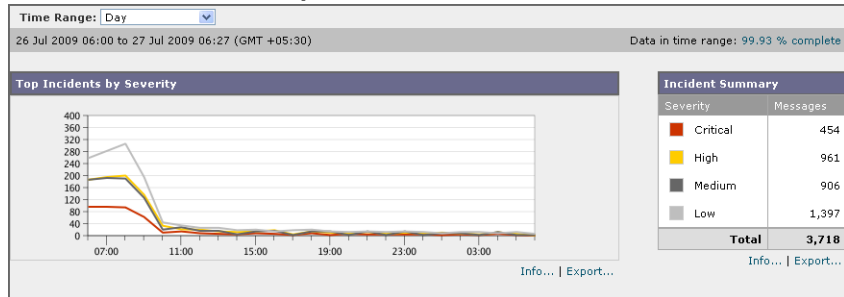
Figure 2-24   DLP Policy Incidents by Sender

Clicking on the sender name opens up the Internal Users page. See The Internal Users Page, page 2-40 for more information.

The Content Filters Page

The Content Filters page shows information about the top incoming and outgoing content filter matches (which content filter had the most matching messages) in two forms: a bar chart and a listing. Using the Content Filters page, you can review your corporate policies on a per-content filter or per-user basis and answer questions like:

- Which content filter is being triggered the most by incoming or outgoing mail?

- Who are the top users sending or receiving mail that is triggering a particular content filter?

You can click the name of the content filter in the listing to view more information about that filter on the Content Filter detail page.

Content Filter Details

The Content Filter detail page displays matches for that filter over time, as well as matches by internal user.

In the Matches by Internal User section, you can click the name of a user to view that internal user's (email address) Internal User details page (see Internal User Details, page 2-40).

Figure 2-25   Content Filters Page
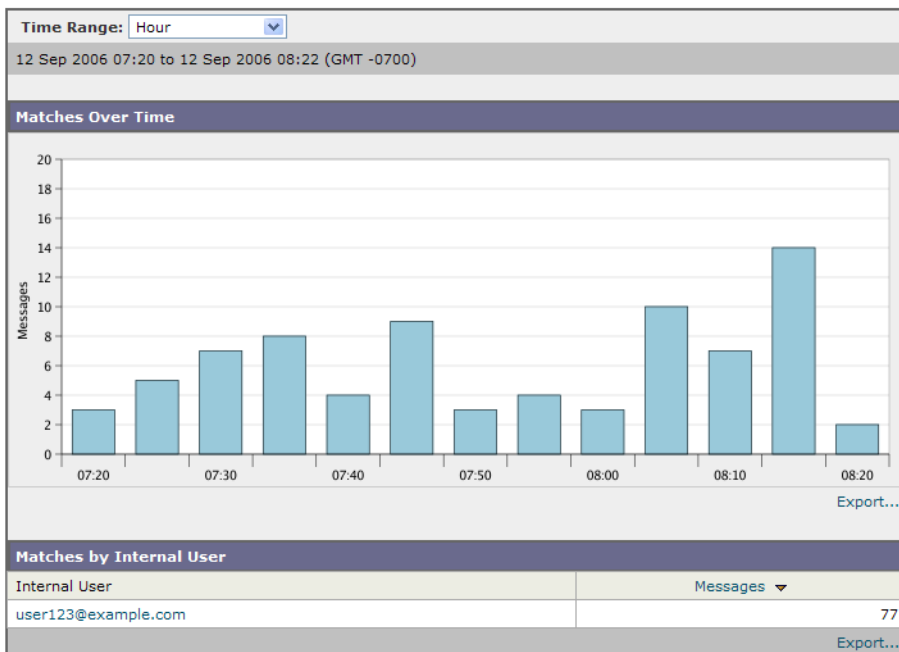
The Virus Outbreaks Page

The Virus Outbreaks page shows the current status and configuration of Virus Outbreak Filters on your IronPort appliance as well as information about recent outbreaks and messages quarantined due to Virus Outbreak Filters. You can use this page to monitor your defense against virus attacks.

The Current Status section provides information about your current Virus Outbreak Filters configuration (if you have licensed and enabled the Virus Outbreak Filters feature). Global outbreak data is automatically downloaded from the IronPort Threat Operations Center once an hour. Note that your IronPort appliance must be able to communicate with downloads.ironport.com in order to correctly populate the tables on this page.

The Outbreak Summary lists global as well as local outbreaks, allowing you to compare local network virus trends to global trends. The listing of global outbreaks is a superset of all outbreaks, whereas local outbreaks are limited to those that have affected your IronPort appliance. Global outbreak data represents all outbreaks detected by the IronPort Threat Operations Center which exceeded the currently configured threshold for the outbreak quarantine. Local outbreak data represents all outbreaks detected on this appliance which exceeded the currently configured threshold for the outbreak quarantine. The Average Protection Time is always based on the difference between when each threat was detected by the IronPort Threat Operations Center and the release of an anti-virus signature by a major vendor. Note that not every global outbreak affects your IronPort appliance. A value of "--" indicates either a protection time does not exist, or the signature times were not available from the anti-virus vendors (some vendors may not report signature times). This does not indicate a protection time of zero, rather it means that the information required to calculate the protection time is not available.

The Quarantined Messages section summarizes Virus Outbreak Filters quarantining, and is a useful gauge of how many potential threat messages Virus Outbreak Filters are catching. Quarantined messages are counted at time of release. Typically, messages will be quarantined before anti-virus signatures are available. When released, they will be scanned by the anti-virus software and determined to be virus positive or clean. If anti-virus software is not enabled on the IronPort appliance, the number of virus positive messages detected will always be zero. Because of the dynamic nature of Virus Outbreak tracking, the rule under which a message is quarantined (and even the associated outbreak) may change while the message is in the quarantine. Counting the messages at the time of release (rather than the time of entry into the quarantine) avoids the confusion of having counts that increase and decrease.

The Outbreak Details listing displays information about specific outbreaks, including the ID, the time and date the outbreak was first seen globally, the lead time provided by Virus Outbreak filters, and the number of quarantined messages. You can select either global or local outbreaks as well as the number of messages to display via the menu on the left. You can sort the listing by clicking on the column headers.

The First Seen Globally time is determined by the IronPort Threat Operations Center, based on data from SenderBase, the world's largest email and web traffic monitoring network. The Virus Outbreak Filters Protection time is based on the difference between when each threat was detected by the IronPort Threat Operations Center and the release of an anti-virus signature by a major vendor.

A value of "--" indicates either a protection time does not exist, or the signature times were not available from the anti-virus vendors (some vendors may not report signature times). This does not indicate a protection time of zero. Rather, it means that the information required to calculate the protection time is not available.

Using the Virus Outbreaks page, you can answer questions like:

- How many messages are being quarantined and by which Virus Outbreak Filter rule?

- How much lead time has the Virus Outbreak Filter feature been providing for virus outbreaks?

- How do my local virus outbreaks compare to the global outbreaks?

Figure 2-26   Virus Outbreaks Page

Virus Types Page

The Virus Types page provides an overview of the viruses entering and being sent from your network. The Virus Types page displays the viruses that have been detected by the virus scanning engines running on your IronPort appliance. You might want to use this report to take a specific action against a particular virus.

For example, if you see that you are receiving a high volume of a viruses known to be embedded in PDF files, you might want to create a filter action to quarantine messages with PDF attachments.

If you run multiple virus scanning engines, the Virus Types page includes results from all enabled virus scanning engines. The name of the virus displayed on the page is a name determined by the virus scanning engines. If more than one scanning engine detects a virus, it is possible to have more than one entry for the same virus.

The Virus Types page gives you an overview of the viruses entering or being sent from or to your network. The Top Incoming Virus Detected section shows a chart view of the viruses that have been sent to your network in descending order. The Top Outgoing Virus Detected section shows a chart view of the viruses that have been sent from your network in descending order.

Note   To see which hosts sent virus-infected messages to your network, you can go to the Incoming Mail page, specify the same reporting period and sort by virus-positive. Similarly, to see which IP addresses have sent virus-positive email within your network, you can view the Outgoing Senders page and sort by virus-positive messages.

Figure 2-27   *Virus Types Page*
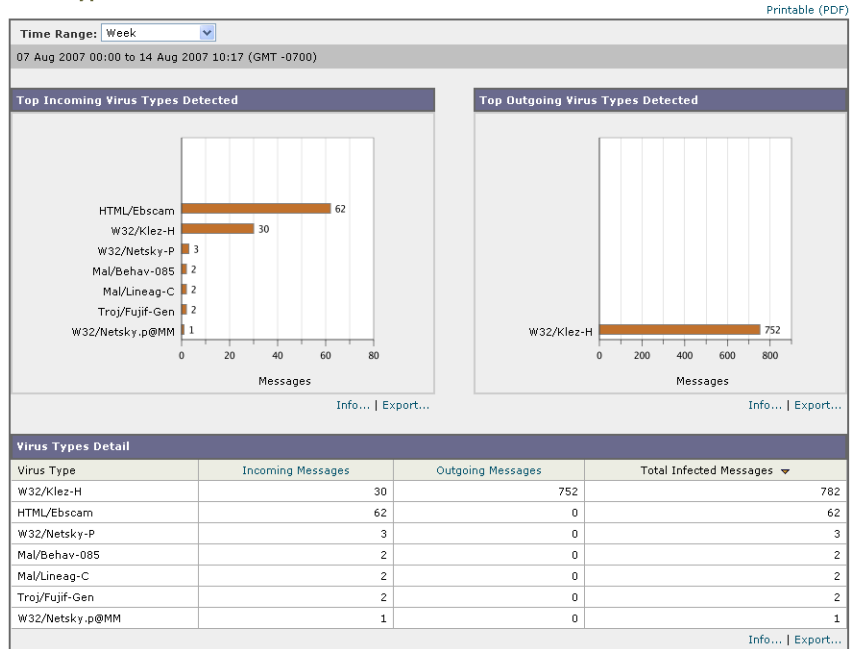
The VirusTypes Details listing displays information about specific viruses, including the infected incoming and outgoing messages, and the total infected messages. The details listing for infected incoming messages displays the name of the virus and the number of incoming messages infected with this virus. Similarly, the outgoing messages displays the name of the virus and the number of outgoing messages infected with the virus. You can sort the Virus Type details by Incoming Messages, Outgoing Messages, or Total Infected Messages.

TLS Connections Page

The TLS Connections pages shows the overall usage of TLS connections for sent and received mail. The report also shows details for each domain sending mail using TLS connections.

The TLS Connections page can be used to determine the following information:

- Overall, what portion of incoming and outgoing connections use TLS?

- What partners do I have successful TLS connections with?

- What partners do I have unsuccessful TLS connections with?
- What partners have issue with their TLS certificates?
- What percent of overall mail with a partner uses TLS?

The TLS Connections page is divided into two sections: a graph and table for incoming connections, and a graph and table for outgoing connections.

The graph displays a view of incoming or outgoing TLS encrypted and non-encrypted connections over the last hour, day, or week. The graph displays the total volume of messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed TLS encrypted messages.

The table displays details for domains sending or receiving encrypted messages. For each domain, you can view the total number of connections, messages sent, and the number of TLS connections that were successful or failed. You can also view the percentage of successful and failed connections for each domain.

Figure 2-28   TLS Connections Report-Incoming Connections
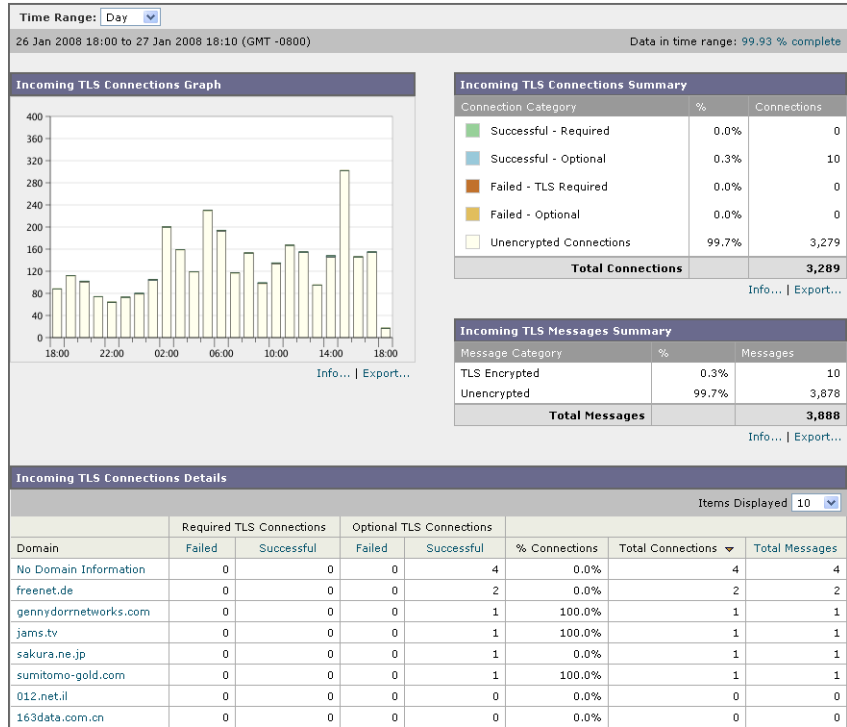
Figure 2-29   TLS Connections Report-Outgoing Connections

Outgoing TLS Connections Graph

Connection Category		%	Connections
Outgoing TLS Connections Summary			
■	Successful - Required	0.0%	0
■	Successful - Optional	100.0%	77
■	Failed - TLS Required	0.0%	0
■	Failed - Optional	0.0%	0
□	Unencrypted Connections	0.0%	0
	Total Connections		**77**

Info... | Export...

Outgoing TLS Messages Summary

Message Category	%	Messages
TLS Encrypted	0.5%	157
Unencrypted	99.5%	28.6k
Total Messages		**28.8k**

Info... | Export...

Outgoing TLS Connections Details

Items Displayed 10

Domain	Required TLS Connections Failed	Required TLS Connections Successful	Optional TLS Connections Failed	Optional TLS Connections Successful	% Connections	Total Connections ▼	Total Messages
No Domain Information	0	0	0	44	100.0%	44	108
t-systems.com	0	0	0	4	100.0%	4	2
ironport.fr	0	0	0	3	100.0%	3	6
lordabbett.com	0	0	0	3	100.0%	3	3
headtechnology.de	0	0	0	2	100.0%	2	4
a-star.edu.sg	0	0	0	1	100.0%	1	1
accusys.com	0	0	0	1	100.0%	1	1
avantec.ch	0	0	0	1	100.0%	1	1
avl.com.cn	0	0	0	1	100.0%	1	1
bmcjax.com	0	0	0	1	100.0%	1	1

Info... | Export...

The System Capacity Page

The System Capacity page provides a detailed representation of the system load, including messages in the work queue, average time spent in the work queue, incoming and outgoing messages (volume, size, and number), overall CPU usage, CPU usage by function, and memory page swapping information.

The system capacity page can be used to determine the following information:

- Identify when an IronPort appliance is exceeding recommended capacity and configuration optimization or additional appliances are needed.

- Identify historical trends in system behavior which point to upcoming capacity issues.

- Identify which part of the system is using the most resources to assist with troubleshooting.

It is important to monitor your IronPort appliance to ensure that your capacity is appropriate to your message volumes. Over time, volume will inevitably rise and appropriate monitoring will ensure that additional capacity or configuration changes can be applied proactively. The most effective way to monitor system capacity is to track overall volume, messages in the work queue and incidents of Resource Conservation Mode.

- **Volume**: It is important to have an understanding of the "normal" message volume and the "usual" spikes in your environment. Track this data over time to measure volume growth. You can use the Incoming Mail and Outgoing Mail pages to track volume over time. For more information, see System Capacity- Incoming Mail, page 2-58 and System Capacity-Outgoing Mail, page 2-59.

- **Work Queue**: The work queue is designed to work as a "shock absorber"-- absorbing and filtering spam attacks and processing unusual increases in ham messages. However, the work queue is also the best indicator of a system under stress, prolonged and frequent work queue backups may indicate a capacity problem. You can use the WorkQueue page to track the average time messages spend in the work queue and the activity in your work queue. For more information, see System Capacity- Workqueue, page 2-56.

- **Resource Conservation Mode**: When an IronPort appliance becomes overloaded, it will enter "Resource Conservation Mode" (RCM) and send a CRITICAL system alert. This is designed to protect the device and allow it to process any backlog of messages. Your IronPort appliance should enter RCM infrequently and only during a very large or unusual increase in mail volume. Frequent RCM alerts may be an indication that the system is becoming overloaded. Resource Conservation Mode is not tracked by the system capacity page.

System Capacity- Workqueue

The Workqueue page shows the average time a message spends in the work queue, excluding any time spent in the IronPort Spam quarantine or in a system quarantine. You can view time periods from an hour up to one month. This average can help in identifying both short term events delaying mail delivery and identify long term trends in the workload on the system.

Note   If a message is released from the quarantine into the work queue, the "average time in work queue" metric ignores this time. This prevents double-counting and distorted statistics due to extended time spent in a quarantine.

The report also shows the volume of messages in the work queue over a specified time period, and it shows the maximum messages in the work queue over the same time period.

Occasional spikes in the Workqueue graphs are normal and expected. If the spikes occur with increasing frequency and are maintained over a long period of time, this may indicate a capacity issue. When reviewing the work queue page, you may want to measure the frequency of work queue backups, and take note of work queue backups that exceed 10,000 messages.

Figure 2-30   System Capacity - Workqueue
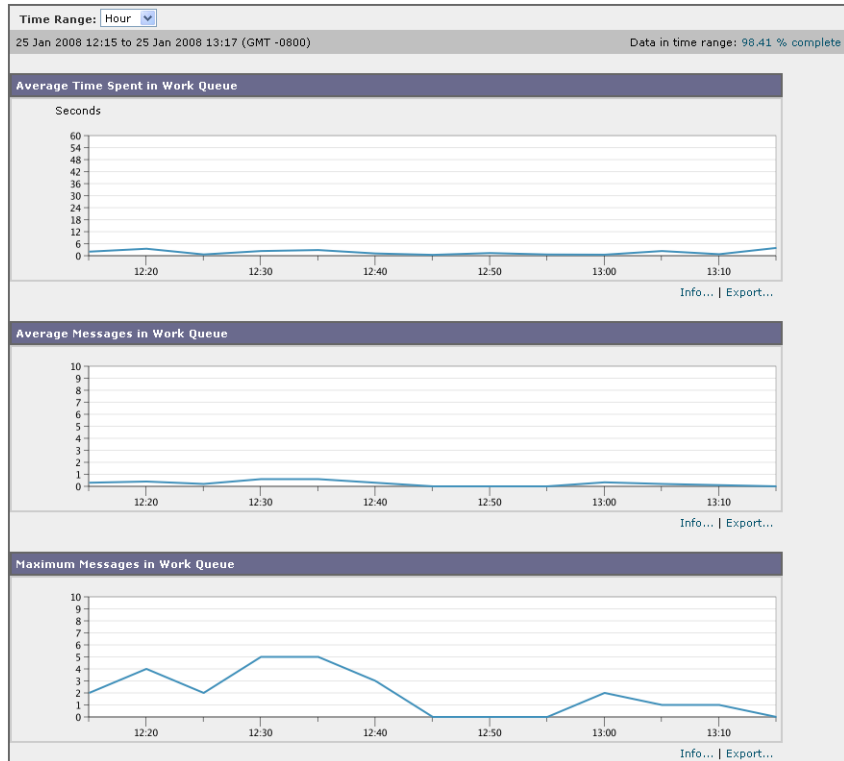
System Capacity- Incoming Mail

The incoming mail page shows incoming connections, the total number of incoming messages, the average message size, and the total incoming message size. You can limit the results by an hour, day, week, or month. It is important to have an understanding of the trends of normal message volume and spikes in your environment. You can use the incoming mail page to help track volume growth over time and plan for system capacity. You might also want to compare the Incoming Mail data with the Sender Profile data to view the trends in volumes of emails that are being sent from specific domains to your network.

Note   an increased number of incoming connections may not necessarily affect system load.

Figure 2-31   System Capacity - Incoming Mail (Page 1 of 2)
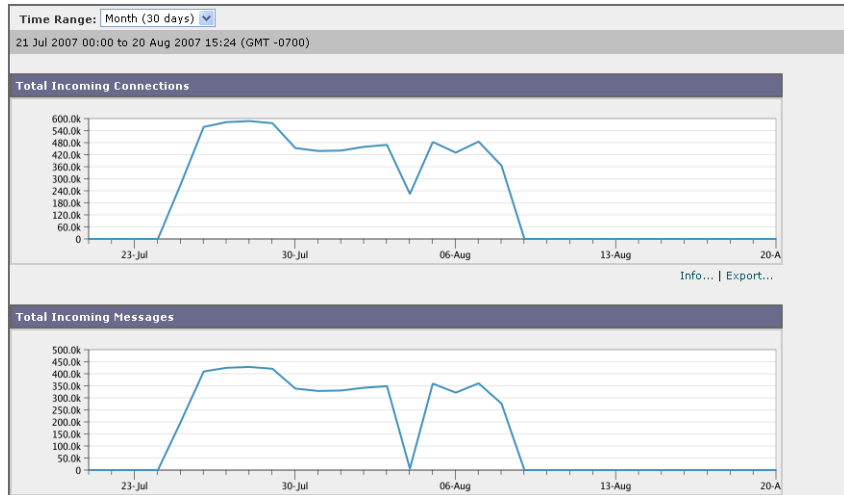
Figure 2-32   System Capacity - Incoming Mail (Page 2 of 2)
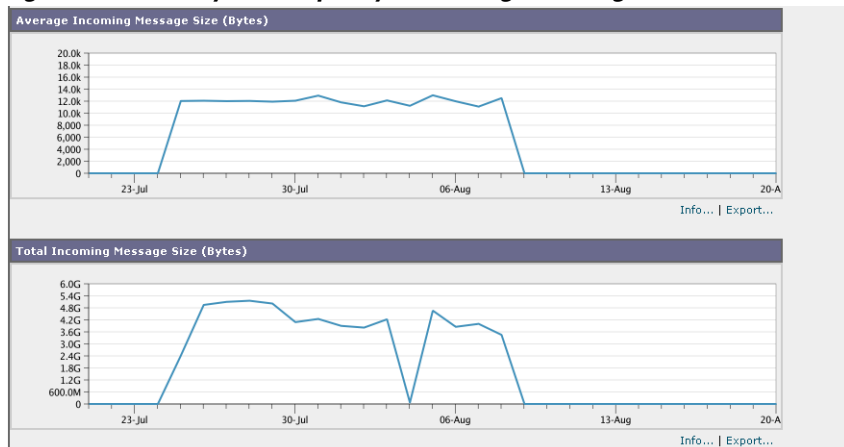
System Capacity-Outgoing Mail

The outgoing mail page shows outgoing connections, the total number of
outgoing messages, the average message size, and the total outgoing message
size. You can limit the results by an hour, day, week, or month. It is important to
have an understanding of the trends of normal message volume and spikes in your

environment. You can use the outgoing mail page to help track volume growth over time and plan for system capacity. You might also want to compare the Outgoing Mail data with the Outgoing Destinations data to view the trends in volumes of emails that are being sent from specific domains or IP addresses.

Figure 2-33   System Capacity - Outgoing Mail (page 1 of 2)
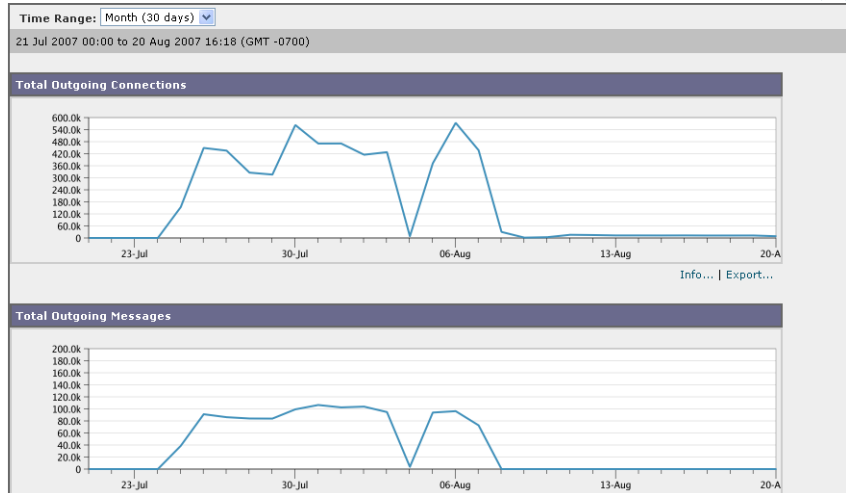
Figure 2-34   System Capacity - Outgoing Mail (page 2 of 2)
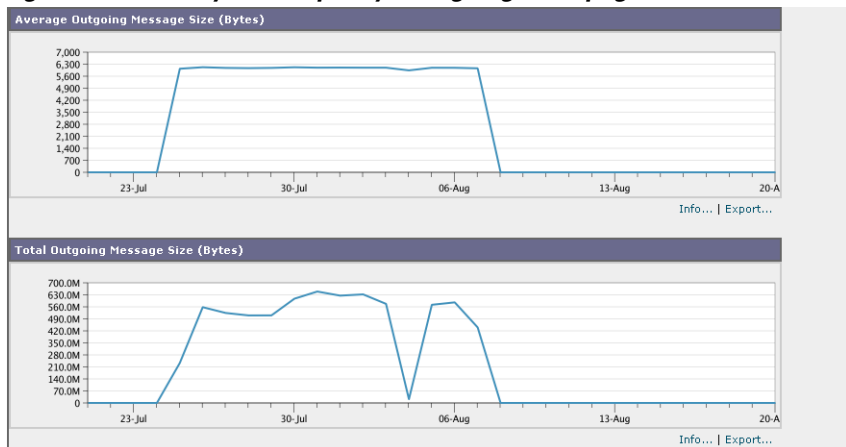
System Capacity-System Load

The system load report shows the overall CPU usage on your IronPort appliance. AsyncOS is optimized to use idle CPU resources to improve message throughput.

High CPU usage may not indicate a system capacity problem. If the high CPU usage is coupled with consistent, high-volume memory page swapping, you may have a capacity problem. This page also shows a graph that displays the amount of CPU used by different functions, including mail processing, spam and virus engines, reporting, and quarantines. The CPU-by-function graph is a good indicator of which areas of the product use the most resources on your system. If you need to optimize your appliance, this graph can help you determine which functions may need to be tuned or disabled.

The memory page swapping graph shows how frequently the system must page to disk.

Figure 2-35   System Capacity - System Load
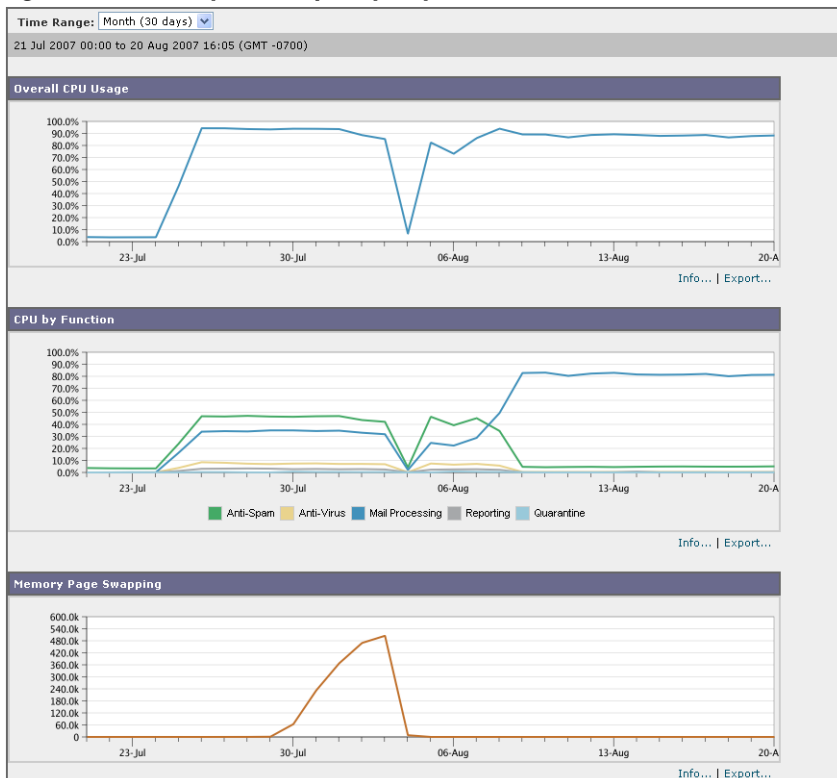
Note about Memory Page Swapping

The system is designed to swap memory regularly, so some memory swapping is expected and is not an indication of problems with your appliance. Unless the system *consistently* swaps memory in high volumes, memory swapping is normal and expected behavior (especially on C10/C100/C150 appliances). For example, Figure 2-36 shows a system that consistently swaps memory in high volumes. To improve performance, you may need to add IronPort appliances to your network or tune your configuration to ensure maximum throughput.

Figure 2-36   System Capacity - System Load (System Under Heavy Load)
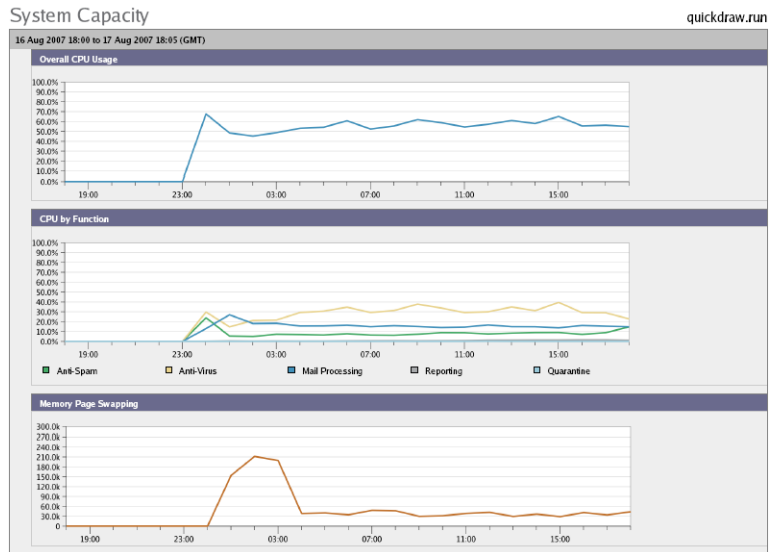
System Capacity- All

The All page consolidates all the previous system capacity reports onto a single page so you can view the relationship between the different reports. For example, you might view the message queue is high at the same time that excessive memory swapping takes place. This might be an indication that you have a capacity problem. You may want to save this page as PDF to preserve a snapshot of system performance for later reference (or to share with support staff).

The System Status Page

The **System Status** page provides a detailed representation of all real-time mail and DNS activity for the system. The information displayed is the same information that is available by using the status detail and dnsstatus commands in the CLI. For more information, see "Monitoring Detailed Email Status" for the status detail command and "Checking the DNS Status" for the dnsstatus command in Chapter 6, "Managing and Monitoring via the CLI."

The System Status page is comprised of four sections: System Status, Gauges, Rates, and Counters.

System Status

The system status section shows Mail System Status and Version Information.

Mail System Status

The Mail System Status section includes:

- System Status (for more information about system status, see Status, page 2-14)

- The last time the status was reported.

- The uptime for the appliance.

- The oldest message in the system, including messages that have not yet been queued for delivery.

Version Information

The Version Information section includes:

- The Cisco IronPort appliance model name.

- The version and build date of the IronPort AsyncOS operating system installed.

- The installation date of the IronPort AsyncOS operating system.

- The serial number of the system to which you are connected.

This information is useful if you are contacting IronPort Customer Support. (See IronPort Customer Support, page 1-7.)

Figure 2-37   *System Status*

System Status	
Mail System Status	Version Information
System Status: Online Status as of: 26 Oct 2006 09:15 (GMT -0700) Up Since: 25 Oct 2006 23:18 (GMT -0700) (9h 57m 36s) Oldest Message: 3 days 33 mins 40 secs	Model: C600 Operating System: 5.0.0-132 Build Date: 24 Oct 2006 00:00 (GMT -0700) Install Date: 25 Oct 2006 23:20 (GMT -0700) Serial Number: XXXXXXXXXXXX-XXXXXXX

Gauges

The Gauges section shows queue and resource utilization.

- Mail Processing Queue

- Active Recipients in Queue

- Queue Space

- CPU Utilization

    Mail Gateway Appliance refers to the percentage of the CPU that AsyncOS processes are consuming. CASE refers to several items, including the IronPort Anti-Spam scanning engine and Virus Outbreak Filters processes.

- General Resource Utilization

- Logging Disk Utilization

Figure 2-38   Gauges

Gauges					
Mail Processing Queue			**CPU Utilization**		
Current Incoming Connections	24		Mail Gateway Appliance	47.0%	
Current Outgoing Connections	34		Symantec Brightmail Anti-Spam	0.0%	
			Anti-Virus	5.0%	
Active Messages in Work Queue	683		Context Adaptive Scanning Engine (CASE)	47.0%	
Active Messages in Quarantine	28.7k		**Total CPU Utilization:**	**99.0%**	
Active Destination Objects in Memory	11.7k				
			General Resource Utilization		
Active Recipients in Queue			RAM Utilization	20.0%	
Unattempted	8,611		Disk I/O Utilization	14.0%	
Attempted	28				
Total Active Recipients:	**8,639**		**Logging Disk Utilization**		
			Logging Disk Utilization	8.0%	
Queue Space			Logging Disk Available	150G	
Queue Space Used by Quarantine	536957K				
Total Queue Space Used	590898K				
Total Queue Utilization	0.8%				

Rates

The Rates section shows rate handling for recipients.

- Mail Handling Rates
- Completion Rates

Figure 2-39   Rates

Rates (Events per Hour)					
Mail Handling Rates	Event Type		1-Minute	5-Minutes	15-Minutes
Receiving	Messages Received		28.6k	27.8k	28.2k
	Recipients Received		51.3k	46.4k	46.6k
Queue	Soft Bounce Events		957	754	791
Completion Rates					
Completed Recipients	Hard Bounce Recipients		311	381	448
	Delivered Recipients		23.9k	24.7k	25.9k
	Total Completed Recipients:		**31.5k**	**32.8k**	**36.3k**

Counters

You can reset the cumulative email monitoring counters for system statistics and view the last time the counters were reset. The reset affects system counters as well as per-domain counters. The reset does not affect the counters on messages in the delivery queue related to retry schedules.

> **Note**   Only user accounts that are in the administrator or operator group have access to reset the counters. User accounts you create in the guest group will not be able to reset the counters. For more information, see Adding Users, page 8-324.

Click Reset Counters to reset the counters. This button offers the same functionality as the `resetcounters` command in the CLI. For more information, see Resetting Email Monitoring Counters, page 6-257.

- Mail Handling Events
- Completion Events
- Domain Key Events
- DNS Status

Figure 2-40   *Counters*

Counters				
		Last Counter Reset:	Never	Reset Counters
Mail Handling Events	**Event Type**	**Reset**	**Uptime**	**Lifetime**
Receiving	Messages Received	17.4M	234.5k	17.4M
	Recipients Received	33.6M	409.4k	33.6M
	Generated Bounce Recipients	699.1k	10.6k	699.1k
Rejection	Rejected Recipients	10.4M	114.3k	10.4M
	Dropped Messages	78.7k	2,492	78.7k
Queue	Soft Bounce Events	893.1k	9,251	893.1k
Completion Events				
Hard Bounce Recipients	DNS Hard Bounces	1,155	114	1,155
	5XX Hard Bounces	535.5k	5,534	535.5k
	Expired Hard Bounces	78.8k	1	78.8k
	Filter Hard Bounces	0	0	0
	Other Hard Bounces	0	0	0
	Total Hard Bounces:	**615.5k**	**5,649**	**615.5k**
Deleted	Deleted Recipients	14.4M	122.4k	14.4M
	Global Unsubscribe Hits	0	0	0
Delivered	Delivered Recipients	23.0M	243.9k	23.0M
	Total Completed Recipients:	**38.0M**	**371.9k**	**38.0M**
Domain Key Events				
Signed Messages	Signed Messages Delivered	0	0	0
DNS Status				
DNS Status	DNS Requests	55.4M	575.5k	55.4M
	Network Requests	55.8M	567.5k	55.8M
	Cache Hits	534.4M	6.2M	534.4M
	Cache Misses	248.2M	2.6M	248.2M
	Cache Exceptions	6.6M	70.0k	6.6M
	Cache Expired	1.2M	2,763	1.2M

Retrieving CSV Data

You can retrieve the data used to build the charts and graphs in the Email Security Monitor in CSV format. The CSV data can be accessed in two ways:

- **CSV reports delivered via email**. You can generate a CSV report that is delivered via email or archived. This delivery method is useful when you want separate reports for each table represented on an Email Security Monitor page, or when you want to send CSV data to users who do not have access to internal networks.

The comma-separated values (CSV) Report Type is an ASCII text file which contains the tabular data of the scheduled report. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file will be created for each table. Multiple CSV files for a single report will be compressed into a single .zip file for the archived file storage option or will all be attached to separate e-mail messages for e-mail delivery.

For information about configuring scheduled or on-demand reports, see Reporting Overview, page 2-72.

- **CSV files retrieved via HTTP**. You can retrieve the data used to build the charts and graphs in the Email Security Monitor feature via HTTP. This delivery method is useful if you plan to perform further analysis on the data via other tools. You can automate the retrieval of this data, for example, by an automatic script that will download raw data, process, and then display the results in some other system.

Retrieving CSV Data Via Automated Processes

The easiest way to get the HTTP query you will need is to configure one of the Email Security Monitor pages to display the type of data you want. You can then copy the **Export** link. This is the download URL. When automating data retrieval like this it is important to note which parameters in the download URL should be fixed and which should change (see below).

The download URL is encoded in such a way that it can be copied to an external script that can execute the same query (using proper HTTP authentication) and get a similar data set. The script can use Basic HTTP Authentication or cookie authentication. Keep the following in mind when retrieving CSV data via automated processes:

- Time range selection (past hour, day, week, etc) in relation to when the URL is used again. If you copy the URL to retrieve a CSV data set for "Past Day," the next time you use that URL you will get a new data set that covers the "Past Day" from the time you send the URL again. The date range selection is retained, and appears in the CSV query string (e.g. `date_range=current_day`).

- Filtering and grouping preferences for the data set. Filters are retained and appear in the query string. Note that filters in reports are rare — one example is the "Global / Local" outbreaks selector in the Virus Outbreaks report.

- The CVS download returns all rows of data in the table for the selected time range.

- The CSV download returns the rows of data in the table ordered by timestamp and key. You can perform further sorting in a separate step such as via a spreadsheet application.

- The first row contains column headers that match the display names shown in the report. Note that timestamps (see Timestamps, page 2-71) and keys (see Keys, page 2-72) also appear.

Sample URL

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

Adding Basic HTTP Authentication credentials

To specify basic HTTP Authentication credentials to the URL:

http://example.com/monitor/

becomes:

http://username:password@example.com/monitor/

File Format

The downloaded file is in CSV format and has a .csv file extension. The file header has a default filename, which starts with the name of the report, then the section of the report.

Timestamps

Exports that stream data show begin and end timestamps for each raw "interval" of time. Two begin and two end timestamps are provided — one in numeric format and the other in human-readable string format. The timestamps are in GMT time, which should make log aggregation easier if you have appliances in multiple time zones.

Note that in some rare cases where the data has been merged with data from other sources, the export file does not include timestamps. For example, the Virus Outbreak Details export merges report data with Threat Operations Center (TOC) data, making timestamps irrelevant because there are no intervals.

Keys

Exports also include the report table key(s), even in cases where the keys are not visible in the report. In cases where a key is shown, the display name shown in the report is used as the column header. Otherwise, a column header such as "key0," "key1," etc. is shown.

Streaming

Most exports stream their data back to the client because the amount of data is potentially very large. However, some exports return the entire result set rather than streaming data. This is typically the case when report data is aggregated with non-report data (e.g. Virus Outbreaks Detail.)

Reporting Overview

Reporting in AsyncOS involves three basic actions:

- You can create Scheduled Reports to be run on a daily, weekly, or monthly basis.
- You can generate a report immediately ("on-demand" report).
- You can view archived versions of previously run reports (both scheduled and on-demand).

Configure scheduled and on-demand reports via the Monitor > Scheduled Reports page. View archived reports via the Monitor > Archived Reports page.

Your IronPort appliance will retain the most recent reports it generates, up to 1000 total versions for all reports. You can define as many recipients for reports as you want, including zero recipients. If you do not specify an email recipient, the system will still archive the reports. If you need to send the reports to a large number of addresses, however, it may be easier to create a mailing list rather than listing the recipients individually.

By default, the appliance archives the twelve most recent reports of each scheduled report. Reports are stored in the /saved_reports directory of the appliance. (See Appendix A, "Accessing the Appliance" for more information.)

Scheduled Report Types

You can choose from the following report types:

- Content Filters
- Delivery Status
- DLP Incident Summary
- Executive Summary
- Incoming Mail Summary
- Internal Users Summary
- Outgoing Destinations
- Outgoing Mail Summary
- Outgoing Senders: Domains
- Sender Groups
- System Capacity
- TLS Connections
- Virus Outbreaks
- Virus Types

Each of the reports consists of a summary of the corresponding Email Security Monitor page. So, for example, the Content Filters report provides a summary of the information displayed on the Monitor > Content Filters page. The Executive Summary report is based on the Monitor > Overview page.

Notes on Reports

Content Filter reports in a PDF format are limited to a maximum of 40 content filters. You can obtain the full listing via reports in a CSV format.

Setting the Return Address for Reports

To set the return address for reports, see the "System Administration" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*. From the CLI, use the addressconfig command.

Managing Reports

You can create, edit, delete, and view archived scheduled reports. You can also run a report immediately (on-demand report). The following report types are available: Content Filters, DLP Incident Summary, Executive Summary, Incoming Mail Summary, Internal Users Summary, Outgoing Mail Summary, Sender Groups, and Virus Outbreaks. Managing and viewing these reports is discussed below.

Note When in Cluster Mode, you are unable to view reports. You may view reports when in machine mode.

The Monitor > Scheduled Reports page shows a listing of the scheduled reports already created on the appliance.

Scheduled Reports

Scheduled reports can be scheduled to run on a daily, weekly, or monthly basis. You can select time at which to run the report. Regardless of when you run a report, it will only include the data for the specified period (previous day, week or month). So, a daily report scheduled to run at 1AM will contain data for the previous day, midnight to midnight.

Your IronPort appliance ships with a default set of scheduled reports —you can use, modify, or delete any of them.

Creating a Scheduled Report

To create a scheduled report,

Step 1   On the Monitor > Scheduled Reports page, click **Add Scheduled Report**. The Add Scheduled Report page is displayed.

Figure 2-41   ***Adding a Scheduled Report***

Add Scheduled Report

Report Settings	
Type:	Select report type... ⌄
Title:	
Time Range To Include:	Previous 7 calendar days ⌄
Format:	● PDF
	○ CSV ⓘ
Schedule:	○ Daily At time: 01 ⌄ : 00 ⌄
	● Weekly on Sunday ⌄
	○ Monthly *on first day of month*
Email to:	
	Separate multiple addresses with commas. Leave blank for archive only.

Cancel   Submit

Step 2   Select a report type. Depending on the report type you select, different options may be available.

For more information about the available types of scheduled reports, see Scheduled Report Types, page 2-73.

Step 3   Enter a descriptive title for the report. AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.

Step 4   Select a time range for the report data. (This option is not available for Virus Outbreak reports.)

Step 5   Select a format for the report:

   – **PDF**. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.

   – **CSV**. Create an ASCII text file that contains the tabular data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.

Step 6   Specify the report options, if available. Some reports do not have report options.

Step 7   Specify scheduling and deliver options. If you do not specify an email address, the report is archived but is not sent to any recipients.

> ✎
>
> **Note**   If you are sending reports to an external account (such as Yahoo or Gmail, etc.), you may need to add the reporting return address to the external account's whitelist to prevent report emails from being incorrectly classified as spam.

Step 8   Click **Submit**. Commit your changes.

Editing Scheduled Reports

To edit a scheduled report:

Step 1   Click the report title in the listing on the Services > Centralized Reporting page.

Step 2   Make your changes.

Step 3   Submit and commit your changes.

Deleting Scheduled Reports

To delete a scheduled report:

Step 1   On the Services > Centralized Reporting page, select the check boxes corresponding to the reports that you want to delete.

> ✎
>
> **Note**   Select the All check box to remove all scheduled reports.

Step 2   Click **Delete**.

Step 3   Confirm the deletion and then commit your changes.

Any archived versions of deleted reports are *not* automatically deleted.

Archived Reports

The Monitor > Archived Reports page lists the available archived reports. You can view a report by clicking its name in the Report Title column. You can generate a report immediately by clicking **Generate Report Now**

Use the Show menu to filter which type of reports is listed. Click the column headings to sort the listing.

Archived reports are deleted automatically — up to 12 instances of each scheduled report (up to 1000 reports) are kept and as new reports are added, older ones are deleted to keep the number at 1000. The 12 instances limit is applied to each individual scheduled report, not report type.

Figure 2-42   Archived Reports

Archived Reports

Available Reports			Show: All reports
Generate Report Now...			
Report Title	Type	Time Range	Generated on ▼
Virus Outbreaks	Virus Outbreaks	Custom	Thu 19 Oct 2006 17:32 (GMT)
Incoming Mail Summary	Incoming Mail Summary	Calendar Week	Thu 19 Oct 2006 17:31 (GMT)
Executive Summary	Executive Summary	Calendar Week	Thu 19 Oct 2006 17:31 (GMT)
Content Filters	Content Filters	Calendar Week	Thu 19 Oct 2006 17:31 (GMT)

On-Demand Reports

You can generate a report without scheduling it. These on-demand reports are still based on a specified time frame, but they are generated immediately.

To generate a report immediately,

Step 1   Click **Generate Report Now** on the Archived Reports page.

Figure 2-43   Generate Report Dialog

Generate Report

Step 2   Select a report type and edit the title if desired. AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.

For more information about the available types of scheduled reports, see Scheduled Report Types, page 2-73.

Step 3   Select a time range for the report data. (This option is not available for Virus Outbreak reports.)

Step 4   Select a format for the report.

– **PDF**. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.

– **CSV**. Create an ASCII text file that contains the tabular data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.

Step 5   Specify any report options.

Step 6   Select whether to archive the report (if so, the report will shown on the Archived Reports page).

Step 7   Specify whether to email the report and to which email addresses to send the report.

Step 8   Click **Deliver this Report** to generate the report and deliver it to recipients or archive it.

Step 9   Commit your changes.

Tracking Email Messages

This chapter contains the following sections:

Tracking Service Overview

The message tracking service makes it easy to find the status of messages processed by AsyncOS, and you can quickly resolve help desk calls by determining the exact location of a message. You can use message tracking to determine if a particular message was delivered, found to contain a virus, or placed in a spam quarantine — or if it is located somewhere else in the mail stream.

You can enable message tracking on your local IronPort Email Security appliance, or you can enable centralized tracking on an M-Series appliance to track messages for multiple email security appliances. For instructions on enabling centralized tracking, see the *Cisco IronPort AsyncOS for Security Management User Guide* . For instructions for enabling local tracking, see Enabling and Disabling Local Message Tracking, page 3-80.

Instead of having to search through log files using "grep" or similar tools, you can use the flexible tracking interface to locate messages. You can use a variety of search parameters in combination.

Tracking queries can include:

- **Envelope information:** Find messages from particular envelope senders or recipients by entering the text strings to match.

- **Subject header:** Match a text string in the subject line. Warning: Do not use this type of search in environments where regulations prohibit such tracking.

- **Time frame:** Find a message that was sent between specified dates and times.

- **Sender IP address or rejected connections:** Search for messages from a particular IP address, or show rejected connections in the search results.

- **Event Information:** Find messages that match specified events, such as messages flagged as virus positive, spam positive, or suspected spam, and messages that were delivered, hard bounced, soft bounced, or sent to the Virus Outbreak Quarantine.

- **Message ID:** Find messages by identifying the SMTP "Message-ID:" header or the IronPort message ID (MID).

Enabling and Disabling Local Message Tracking

To enable local message tracking:

Step 1   Click Services > Message Tracking.

The Message Tracking page is displayed.

Figure 3-1   *The Message Tracking Page with Local Message Tracking Enabled*

Message Tracking Service Settings

Step 2   In the Message Tracking section, click **Enable Message Tracking Service**.

If you are enabling message tracking for the first time after running the System Setup Wizard, review the end-user license agreement, and click **Accept**.

Step 3   Optionally, select the check box to save information for rejected connections.

Step 4   Submit and commit your changes.

Disabling Local Message Tracking

To disable the local message tracking service:

Step 1   On Services > Message Tracking, click the **Edit Settings** button.

Step 2   Clear the Enable Message Tracking Service check box.

Step 3   Submit and commit your changes.

Understanding Tracking Query Setup

The message tracking service enables administrators to search for a particular email message or group of messages that match specified criteria, such as the message subject line, date and time range, envelope sender or recipient, and processing event (for example, whether the message was virus positive, spam positive, hard bounced, delivered, and so forth). Message tracking gives administrators a detailed view of message flow. You can also "drill down" on particular email messages to see message details, such as the processing events or the envelope and header information.

Note   Although the tracking component provides detailed information about individual email messages, you cannot use it to read the content of messages.

You use the Monitor > Message Tracking page to locate email messages.

Figure 3-2   The Message Tracking Page

Optionally, click the Advanced link to display more options for tracking.

Figure 3-3   Advanced Options for Tracking

Message Tracking

✎

Note   Tracking does not support wildcard characters or regular expressions. Tracking searches are not case sensitive.

You can use the following search parameters when you run a message tracking query:

- **Envelope Sender:** Select "Begins With," "Is," or "Contains," and enter a text string to search for in the envelope sender. Valid parameter values are email addresses, usernames, and domains.

- **Envelope Recipient:** Select "Begins With," "Is," or "Contains," and enter text to search for in the envelope recipient. Valid parameter values are email addresses, usernames, and domains.

  If you use the alias table for alias expansion, the search finds the expanded recipient addresses rather than the original envelope addresses. In all other cases, message tracking queries find the original envelope recipient addresses.

- **Subject:** Select "Begins With," "Is," "Contains," or "Is Empty," and enter a text string to search for in the message subject line.

✎

Note   International character sets are not supported in the subject header.

- **Dates and Times:** Specify a date and time range for the query. If you do not specify a date, the query returns data for all dates. If you specify a time range only, the query returns data for that time range across all available dates.

    Dates and times are converted to GMT format when they are stored in the database. When you view dates and times on an appliance, they are converted to the local time of the appliance.

    Messages appear in the results only after they have been logged. Depending on the size of logs and the frequency of polling, there could be a small gap between the time when an email was sent and when it actually appears in tracking and reporting results. See Chapter 5, "Logging" for more details.

- **Message Event:** Select the events to track. Options are "Virus Positive," "Spam Positive," "Suspect Spam," "Delivered," "Hard Bounced," "Soft Bounced," "Currently in Outbreak Quarantine," "DLP Violations," and "Quarantined as Spam." Unlike most conditions that you add to a tracking query, events are added with an "OR" operator. Selecting multiple events expands the search.

    If you select "DLP Violations," AsyncOS displays additional DLP-related options are displayed. Options are the DLP policy that the messages violated and the severity of the violation ("Critical," "High," "Medium," and "Low").

- **Message-ID Header and MID:** Enter a text string for the "Message-ID:" header, the IronPort message ID (MID), or both.

Running a Search Query

To search for messages by running a query:

Step 1   On the Monitor > Message Tracking page, complete the desired search fields.

For more information about the available search fields, see Understanding Tracking Query Setup, page 3-81.

You do not need to complete every field. Except for the Message Event options, the query is an "AND" search. The query returns messages that match the "AND" conditions specified in the search fields. For example, if you specify text strings for the envelope recipient and the subject line parameters, the query returns only messages that match *both* the specified envelope recipient *and* the subject line.

Step 2   Click **Search** to submit the query. The query results are displayed at the bottom of the page. Each row corresponds to an email message.

Figure 3-4   ***Message Tracking Query Results***

Step 3   If the number of returned rows is greater than the value specified in "Items per page" field, the results are displayed on multiple pages. To navigate through the pages, click the page numbers at the top or bottom of the list.

Step 4   If necessary, refine the search by entering new search criteria, and run the query again. Alternatively, you can refine the search by narrowing the result set, as described in the following section.

Narrowing the Result Set

After you run a query, you might find that the result set includes more information than you need. Instead of creating a new query, you can narrow the result set by clicking a value within a row. Clicking a value adds the parameter value as a condition in the search. For example, if the query results include messages from multiple dates, you can click a particular date within a row to show only messages that were received on that date.

To narrow the result set:

Step 1   Float the cursor over the value that you want to add as a condition. The value is highlighted in yellow.

You can use the following parameter values to refine the search:

 - Date and time
 - Message ID (MID)
 - Sender's username
 - Sender's domain
 - Recipient's username
 - Recipient's domain
 - Subject line of the message

Step 2   Click the value to refine the search.

The Results section displays the messages that match the original query parameters *and* the new condition that you added.

Step 3   If necessary, click additional values in the results to further refine the search.

> **Note**   To remove query conditions, click the Clear button and run a new tracking query.

Understanding Tracking Query Results

Tracking query results list all of the messages that match the criteria specified in the tracking query. Except for the Message Event options, the query conditions are added with an "AND" operator. The messages in the result set must satisfy all of the "AND" conditions. For example, if you specify that the envelope sender begins with J and you specify that the subject begins with T, the query returns a message only if both conditions are true for that message.

For each message, the following information is shown: Date/Time, Sender, Recipient, Subject, Last State, and IronPort message ID (MID). To view detailed information about a message, click the Show Details link for that message. For more information, see Message Details, page 3-87.

> **Note** The Security Management appliance returns up to the first 10,000 rows of data. To access additional records, adjust the query parameters and run a new query.

Message Details

To view detailed information about a particular email message, including the message header information and processing details, click the Show Details link. A new browser window opens with the message details.

Figure 3-5 **Message Details**

The message details include the following sections: Envelope and Header Summary, Sending Host Summary, and Processing Details.

Envelope and Header Summary

This section displays information from the message envelope and header, such as the envelope sender and recipients. It includes the following information:

Received Time: Time that the Email Security appliance received the message.

MID: IronPort message ID.

Subject: Subject line of the message.

The subject line in the tracking results may have the value "(No Subject)" if the message does not have a subject or if the IronPort Email Security appliances are not configured to record the subject lines in log files.

For more information about configuring Email Security appliances to log subject headers, see Chapter 5, "Logging."

Envelope Sender: Address of the sender in the SMTP envelope.

Envelope Recipients: Addresses of the recipients in the SMTP envelope.

Message ID Header: "Message-ID:" header that uniquely identifies each email message. It is inserted in the message when the message is first created. The "Message-ID:" header can be useful when you are searching for a particular message.

SMTP Auth User ID: SMTP authenticated username of the sender, if the sender used SMTP Authentication to send the email. Otherwise, the value is "N/A."

Sending Host Summary

Reverse DNS Hostname: Hostname of the sending host, as verified by reverse DNS (PTR) lookup.

IP Address: IP address of the sending host.

SBRS Score: SenderBase reputation score. The range is from 10 (likely a trustworthy sender) to -10 (apparent spammer). A score of "None" indicates that there was no information about this host at the time the message was processed.

Processing Details

This section displays various logged status events during the processing of the message.

Entries include information about Mail Policy processing, such as Anti-Spam and Anti-Virus scanning, and other events such as message splitting and custom log entries added by a content or message filter.

If the message was delivered, the details of the delivery are displayed here. The last recorded event is highlighted in the processing details.

Quarantines

Quarantines are special queues or repositories used to hold and process messages. IronPort AsyncOS allows you to place incoming or outgoing messages into one of two kinds of quarantines: 'system' and 'IronPort Spam.'

Messages in quarantines can be delivered or deleted. You can create, modify, and delete quarantines. You can associate users with quarantines. You can view the contents of each of your quarantines, search a quarantine for specific messages, and send copies of the messages.

This chapter contains the following sections:

Quarantines Overview

As messages are processed by the IronPort appliance, various actions are applied. Filters are applied to messages, messages are scanned for spam or viruses, and the Virus Outbreak Filters feature scans messages. Any of these actions can cause a message to be quarantined, depending on your settings.

Quarantine Types

An IronPort Spam quarantine is a special kind of quarantine used to hold spam or suspected spam messages for end users. End users are mail users, outside of AsyncOS. You can have a local IronPort Spam quarantine, stored on the IronPort appliance. You can also send messages to an external IronPort Spam quarantine, stored on a separate IronPort appliance. IronPort Spam quarantines can be accessed by both AsyncOS administrators and end users (these are not AsyncOS users).

A system quarantine (unchanged from previous versions) is used to hold messages based on various actions performed by AsyncOS, such as filtering, anti-virus scanning, and Virus Outbreak Filters.

System Quarantines

Typically, messages are placed in system quarantines due to a filter action. Additionally, the Virus Outbreak Filters feature quarantines suspicious messages in the Outbreak quarantine, specifically. System quarantines are configured to process messages automatically—messages are either delivered or deleted based on the configuration settings (for more information, see System Quarantine Settings, page 4-95) set for the quarantine(s) in which the message is placed. In addition to the automated process, designated users (such as your mail administrator, Human Resources personnel, Legal department, etc.) can review the contents of the quarantines and then either release, delete, or send a copy of each message. Released messages are scanned for viruses (assuming that anti-virus is enabled for that particular mail policy).

System Quarantines are ideal for:

- Policy Enforcement - have Human Resources or the Legal department review messages that contain offensive or confidential information before delivering them.

- Virus quarantine - store messages marked as not scannable (or encrypted, infected, etc.) by the anti-virus scanning engine.

- Providing a foundation for the Virus Outbreak Filters feature - hold messages flagged by the Virus Outbreak Filters feature until a virus update is released. For more information about the Virus Outbreak Filters feature, see the "Virus Outbreak Filters" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Your IronPort appliance can have several pre-configured quarantines, depending on features licensed; however, the Policy quarantine is created by default, regardless of license.

- Outbreak, a quarantine used by the Virus Outbreak Filters feature created when the Virus Outbreak Filters feature license key is enabled.

- Virus, a quarantine used by the anti-virus engine, created when the anti-virus license key is enabled.

- Policy, a default quarantine (for example, use this to store messages requiring review).

For details on how to add, modify, or delete additional quarantines, see Managing System Quarantines via the Graphical User Interface (GUI), page 4-94.

Access and interact with system quarantines via the Graphical User Interface (GUI) or the Command Line Interface (CLI) via the quarantineconfig command.

✎
Note   The Command Line Interface (CLI) for system quarantines contains a subset of the functionality found in the GUI (see the *Cisco IronPort AsyncOS CLI Reference Guide*).

IronPort Spam Quarantines

AsyncOS can be configured to send both spam and suspected spam to an IronPort Spam quarantine. You can also configure the system to send a notification email to users, informing them of quarantined spam and suspected spam messages. This notification contains a summary of the messages currently in the IronPort Spam quarantine for that user. The user may view the messages and decide whether to have them delivered to their inbox or delete them. Users can also search through their quarantined messages. Users can access the quarantine via the notification or directly via a web browser (this requires authentication, see Configuring End User Quarantine Access, page 4-123).

The system can be configured to be self-maintaining, meaning that mail is periodically deleted from the IronPort Spam quarantine automatically in order to keep from consuming all of the quarantine space. IronPort Spam quarantines are used specifically to hold spam and suspect spam messages for end users.

For more information about IronPort Spam quarantines, see Managing Messages in IronPort Spam Quarantines, page 4-139.

Managing System Quarantines via the Graphical User Interface (GUI)

Log in to the Graphical User Interface (GUI) and click the Monitor tab. (For information about how to access the GUI, see the "Overview" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.) Click the Quarantines link in the Quarantines section of the left menu.

Figure 4-1   The Quarantines Page

Quarantines

Quarantine	Messages	Default Action	Status	Settings
IronPort Spam Quarantine ▣	0	Retain 14 days then Delete	0% Full	Edit
Outbreak [Manage by Rule Summary]	0	Retain 12 hours then Release	0% Full	Edit
Policy	0	Retain 10 days then Release	0% Full	Edit
Virus *	0	Retain 30 days then Delete	0% Full	Edit

* This Quarantine cannot be used until the related security service is enabled.

The Quarantines page shows information about all of your quarantines, including the number of messages contained in each, the default action (length of time to retain, and then the final action of delete or release), and the percentage full. You can edit the settings (size, retention period, default action, how to handle overflow messages, and users associated with the quarantine) via the Edit link (for more information, see System Quarantine Settings, page 4-95). Also displayed is the status of the quarantine, including whether or not the associated security service

(anti-virus scanning for the Virus quarantine, and Virus Outbreak Filters for the Outbreak quarantine) is enabled, and whether or not the particular quarantine's contents are currently available.

Also note that if the IronPort Spam Quarantine is enabled on the appliance, it is visible in the Quarantines listing. This is an end user quarantine, for more information about working with end user quarantines, see Configuring the IronPort Spam Quarantines Feature, page 4-114.

System Quarantine Settings

Quarantines have an automated process for handling messages based on quarantine settings. Quarantines have several settings used to determine how the quarantine acts on a day-to-day basis: Space Allocation, Retention Time, Default Action, Overflow Messages, and Users. Once you have made a change, click the **Submit** button, add a optional comment if necessary, and then click **Commit Changes** to save the changes.

Allocating Space for System Quarantines

There is a limited amount of space available for system quarantines, as they are created on the IronPort appliance itself. The amount of available space for new quarantines is displayed on the Manage Quarantines page. Messages are forced from the quarantine when the size of the quarantine reaches the space allocated. For more information, see System Quarantine Settings, page 4-95.

Table 4-1   Space Available for Quarantines on IronPort Appliances

IronPort Appliance	Storage Space	Virus Outbreak Filters Storage Space*
X1000/1050/1060	10GB	3GB
C600/650/660	10GB	3GB
C60	5GB	3GB
C300/350/360	4GB	2GB
C30	2GB	2GB
C150/160	2.5GB	1GB
C10/100	1GB	1GB

* Additional space when licensing the Virus Outbreak Filters feature.

The minimum size for a quarantine is 250MB.

Retention Time

Retention Time is the length of time messages are kept in a quarantine. The Default Action (see Default Action, page 4-96) is performed on any message in the quarantine once that retention time is reached. Each message has its own specific expiration time, displayed in the quarantine listing.

Messages are stored for the amount of time specified (Normal Expiration) unless they are manually processed by a mail administrator (or other user) or the size limit set for the quarantine is reached. If the size limit is reached, the oldest messages are processed (Early Expiration) and the Default Action in performed for each message until the size of the quarantine is again less than the size limit. The policy is First In First Out (FIFO). For more information about specifying quarantine size limits, see Creating System Quarantines, page 4-98.

The expiration time on a message can be delayed (extended) via the Select Action menu in the various quarantine listings. Delaying the expiration of a message can be helpful when you need to keep specific messages in the quarantine past their scheduled expiration (for example, waiting for an administrator to have time to review the messages or for a specific anti-virus IDE to be published).

Default Action

The Default Action is the action performed on messages in a quarantine when either of the two following circumstances occur:

- Normal Expiration - the Retention Time is met for a message in the quarantine (see Retention Time, page 4-96).

- Early Expiration - a message is forced from the quarantine when the size limit for the quarantine is reached. For more on setting size limits for quarantines, see Creating System Quarantines, page 4-98. Messages released from quarantine because of a queue-full condition (early expiration) can optionally have other operations performed on them. For more information, see Overflow Messages, page 4-97.

There are two Default Actions:

- Delete - the message is deleted.

- Release - the message is released for delivery. Upon release, the message is rescanned for viruses, assuming anti-virus is enabled for that particular mail policy. For more information about virus scanning and messages released from quarantines, see System Quarantines and Virus Scanning, page 4-112.

Note   In addition to these two default actions, a third message action (Delay Exit) is available in the Select Action menu in the quarantined messages listing.

Overflow Messages

The Overflow Messages section is used to dictate how messages are handled as they are released from the quarantine due to overflow. These settings include: Subject Tagging, Adding an X-Header, and Stripping Attachments.

Subject Tagging

Messages released or deleted from a quarantine because of a queue-full condition (early expiration only) can optionally have their subjects tagged with text you specify when editing or creating a quarantine.

The tag is a user-defined string that can either be prepended or appended to the original subject header.

Note   In order for a subject with non-ASCII characters to display correctly it has to be represented according to RFC 2047.

Add X-Header

Messages released or deleted from a quarantine because of a queue-full condition (early expiration only) can optionally have an X-Header added.

Specify the name of the X-Header and the value.

Strip Attachment

Messages released or deleted from a quarantine because of a queue-full condition (early expiration only) can optionally have their attachments stripped. This can be used to help reduce the chance for virus infected files will be released from a quarantine.

Users and User Groups

Users belonging to the Administrators group have access to quarantines by default. Users in the Operators, Guests, Read-Only Operators, and Help Desk Users groups can be assigned to a quarantine (so that they may view, process, or search messages within a quarantine), but cannot change the quarantine's configuration (e.g. the size, retention period, etc.), or create or delete quarantines.

Creating System Quarantines

You can create new system quarantines to hold messages. The basic workflow for setting up a quarantine is:

1. Create local users that will interact with the quarantine. A quarantine's user list contains local users in all user groups, except Administrators. Users in the Administrators group always have full access to the quarantine. For more information, see Adding Users, page 8-324. You can also enable your IronPort appliance to use an external directory to authenticate users and select which user groups have access to the quarantine. For more information, see External Authentication, page 8-330.

2. Create the quarantine, following the steps below.

3. Create filters that will move messages to the quarantine. For more information about creating filters, see the "Email Security Manager" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* and refer to "Using Message Filters to Enforce Email Policies" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

To create a system quarantine:

Step 1   Click **Add Quarantine** on the Quarantines page. The Add Quarantine page is displayed.

Step 2   Type a name for the quarantine.

Step 3   Specify the space (in megabytes) to allocate for the quarantine. For more information, see Allocating Space for System Quarantines, page 4-95.

Step 4   Select a Retention Period, or time to keep a message in the quarantine before the default action in performed on the message. For more information, see Retention Time, page 4-96.

Step 5   Select a Default Action (Delete or Release).

Step 6   If you want to modify the subject of messages that are processed through the quarantine, type the text to add and select whether to prepend or append it to the original message subject. For more information, see Subject Tagging, page 4-97.

Step 7   If you want to add an X-Header, enter the name and value. For more information, see Add X-Header, page 4-97.

Step 8   If you want to strip any file attachments when the file is release from the quarantine due to overflow (early release), select On. For more information, see Strip Attachment, page 4-98.

Step 9   Select users to associate with this quarantine by clicking on the name of the user. Hold the CTRL key and click to select multiple users. A quarantine's user list contains local users in all user groups, except Administrators. Users in the Administrators group always have full access to the quarantine. For more information, see Users and User Groups, page 4-98. A warning is displayed if you have not yet created any users.

Step 10   Optionally, select the check boxes for the user roles of externally authenticated users to associate with the quarantine. Externally authenticated users are authenticated by your IronPort appliance using a centralized authentication system. For more information, see External Authentication, page 8-330.

Step 11   Submit and commit your changes.

Editing System Quarantines

Only users belonging to the Administrators group can edit quarantines.

To edit an existing quarantine:

Step 1   Click the Edit link in the Settings column for the quarantine you want to modify. The Edit Quarantine page is displayed:

Figure 4-2   Editing a System Quarantine

Step 2   Make your changes to the settings for the quarantine.

Step 3   Submit and commit your changes.

Deleting System Quarantines

To delete an existing quarantine:

Step 1   Click the Delete Quarantine link in the Edit Quarantine page:

Figure 4-3   Deleting a System Quarantine

Edit Policy Quarantine

Settings	
	Delete Quarantine
Quarantine Name:	Policy
Space Allocation:	1024 MB *(Maximum Size 3072 MB)*
Default Action:	Retain 10 Days ▼ then Release ▼
When Allocated Space is Exceeded Send Messages and:	Modify Subject: None ▼
	Add X-Header: Name: X-Quarantine Value: Overflow
	Strip Attachments: ○ No ⦿ Yes
Administrative Users	
You have no 'administrator' or 'operator' users defined for your system. *Go to **System Administration > Users** to configure users.*	

Cancel   Submit

Step 2   A confirmation message is displayed:

Figure 4-4   Confirming a System Quarantine Deletion

Confirm Delete

Are you sure you want to delete "Policy"?

Cancel   Delete

Step 3   Click **Delete**. The quarantine is deleted.

Step 4   Commit your changes.

Working with Messages in System Quarantines

Use the Quarantine Overview to work with messages within quarantines. As a user with access to a quarantine, you can:

- View the messages in a quarantine.

- Perform Message Actions on (process) messages.

- Download message attachments.

- Search for messages in quarantines.

Note The functionality described in this section applies only to the GUI.

Viewing Messages in a System Quarantine

Use the Local Quarantine page to see if a quarantine contains any messages. In this example, the Policy quarantine has 241 messages:

Figure 4-5   Local Quarantines

Quarantines

Quarantine	Messages	Default Action	Status	Settings
IronPort Spam Quarantine	110	Retain 14 days then Delete	0% Full	Edit
Outbreak [Manage by Rule Summary]	0	Retain 12 hours then Release	0% Full	Edit
Policy	241	Retain 10 days then Delete	0% Full	Edit
Virus	0	Retain 30 days then Delete	0% Full	Edit

Click the name of the quarantine to view the messages in the quarantine. From this page, you can view a particular message, process one or more messages, or search through messages.

Processing Messages in a Quarantine

Messages can be removed from quarantines (delivered or deleted) either automatically, through normal or early expiration, or manually.

Manually processing messages means to manually select a Message Action for the message from the Message Actions page.

Click on the quarantine name on the Quarantine Overview page to view the messages in the quarantine:

Figure 4-6   *Viewing the List of Messages in a Quarantine*

All of the messages within the quarantine are listed, including the following information for each message: To, From, Subject, Date Received, Scheduled Exit date, Size, and "In other quarantines." You can navigate through the list of pages using the Previous, Next, page number, or double arrow links. The double arrows take you to the first (<<) or last (>>) page in the listing.

The "In other quarantines" column will contain 'Yes' if the message is present in one or more other quarantines, regardless of whether you have permissions to access those other quarantines. See Multi-User Access and Messages in Multiple Quarantines, page 4-110 for more information.

Sort the results ascending or descending by clicking on any of the column headings (except "In other quarantines").

You can select messages by clicking the corresponding checkbox in the row of checkboxes to the left of the listing. To select all of the messages currently displayed in the listing, mark the All box in the header (the very top of the listing, above the first message). Note that this only applies to the currently displayed messages. Messages not displayed on the current page are not affected.

You can apply an action (Delete, Release, Delay Scheduled Exit) on all selected messages in the listing. Select an action from the pulldown menu at the bottom of the listing and click **Submit**. A dialog box is displayed, asking you to confirm your choice. Click **Yes** to perform the action on all marked messages.

Click the "Manage Rule by Summary" link for the Outbreak quarantine to process the messages in the Outbreak quarantine by rule. For more information, see The Virus Outbreak Filters Feature and the Outbreak Quarantine, page 4-113.

Quarantined Messages and International Character Sets

For messages with subjects containing characters from international character sets (double-byte, variable length, and non-ASCII encoded) the System Quarantine pages display subject lines in non-ASCII characters in their decoded form.

Message Actions and Viewing Message Content

Click on the subject line of a message to view that message's content and to access the Quarantined Message page:

Figure 4-7   Quarantined Message Page

Quarantined Message

Quarantine Details			

Select	Quarantine	Reason	Time Received	Time Scheduled to Exit
☐	Policy	DLP Policy: 'Transmission of Contact Information'	28 Jul 16:25 (GMT +05:30)	07 Aug 16:25 (GMT +05:30)

Select Action...   Submit

< Back to Message List

Message Details

Test for Viruses:	Start Test
Send Copy To:	E-Mail Addresses, comma separated: [ ] Send
Envelope Sender:	user@test.com
Recipients:	user1@test.com
Subject:	DLPTEST

Matched Content

▽ Policy

Attachment Name	Matched Content	Condition
FP1.1.txt	• MS 38930 USA Facilities 662-646-0523 jsamuelson@acmecorp.com 7/17/06 4929132070312710 Acme Corp Irene Gibbs 808 Sumner Street Greenwood MS 38930 USA Publishing 662-646-0522 igibbs@acmecorp.com 2/1/07 4485231592071860 Acme Corp Kathy Lopez 808 Sumner Street Greenwood MS 38930 USA Marketing 662-646-0541 klopez@acmecorp.com 2/1/07 4716298862510192 Acme Corp Marty Smith 808 Sumner Street Greenwood MS 38930 USA Engineering 662-646-0542	DLP Classifier: Contact Information

Headers

```
X-IronPort-AV: E=Sophos;i="4.43,282,1246818600";
   d="txt'?scan'208";a="178202"
Received: from d2.vmw023-bsd04.ibqa (HELO vmw023-bsd04.ibqa) ([172.22.107.1])
   by c360q02.ibqa with ESMTP; 28 Jul 2009 16:25:03 +0530
Message-ID: <792087.518002035-sendEmail@vmw023-bsd04>
From: "user@test.com" <user@test.com>
To: "user1@test.com" <user1@test.com>
Subject: DLPTEST
Date: Tue, 28 Jul 2009 08:42:11 +0000
X-Mailer: sendEmail-1.55
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----MIME delimiter for sendEmail-538525.714612664"
```

Message

Test

Message Parts

Name	Size	Details
[message body]	6	ASCII text, with CRLF line terminators
FP1.1.txt	1K	ASCII text

< Back to Message List

The Quarantined Message page has two sections: Quarantine Details and Message Details.

From the Quarantined Message page, you can read the message, select a Message Action, send a copy of the message, or test for viruses. You can also see if a message will be encrypted upon release from the quarantine due to the Encrypt on Delivery filter action.

The Message Details section displays the message body, message headers, and attachments. Only the first 100K of the message body is displayed. If the message is longer, the first 100K is shown, followed by an ellipsis (...). The actual message is not truncated. This is for display purposes only. You can download the message body by clicking [message body] in the Message Parts section at the bottom of Message Details. You can also download any of the message's attachments by clicking the attachment's filename.

If you view a message that contains a virus and you have desktop anti-virus software installed on your computer, your anti-virus software may complain that it has found a virus. This is not a threat to your computer and can be safely ignored.

Note   For the special Outbreak quarantine, additional functionality is available. See The Virus Outbreak Filters Feature and the Outbreak Quarantine, page 4-113 for more information.

Viewing Matched Content

When you configure a quarantine action for messages that match Attachment Content conditions, Message Body or Attachment conditions, Message body conditions, or the Attachment content conditions, you can view the matched content in the quarantined message. When you display the message body, the matched content is highlighted in yellow, except for DLP policy violation matches. You can also use the $MatchedContent action variable to include the matched content from message or content filter matches in the message subject.

If the attachment contains the matched content, the attachment's contents are displayed as well as the reason it was quarantined, whether it was due to a DLP policy violation, content filter condition, message filter condition, or Image Analysis verdict.

When you view messages in the local quarantine that have triggered message or content filter rules, the GUI may display content that did not actually trigger the filter action (along with content that triggered the filter action). The GUI display

should be used as a guideline for locating content matches, but does not necessarily reflect an exact list of content matches. This occurs because the GUI uses less strict content matching logic than is used in the filters. This issue applies only to the highlighting in the message body. The table that lists the matched strings in each part of the message along with the associated filter rule is correct.

You can download a message attachment by clicking the attachment's file name in the Message Parts or Matched Content section. AsyncOS displays a warning that attachments from unknown sources may contain viruses and asks you if you want to continue. You can also download the message body by clicking `[message body]` in the Message Parts section.

Figure 4-8   Matched Content Viewed in the Policy Quarantine
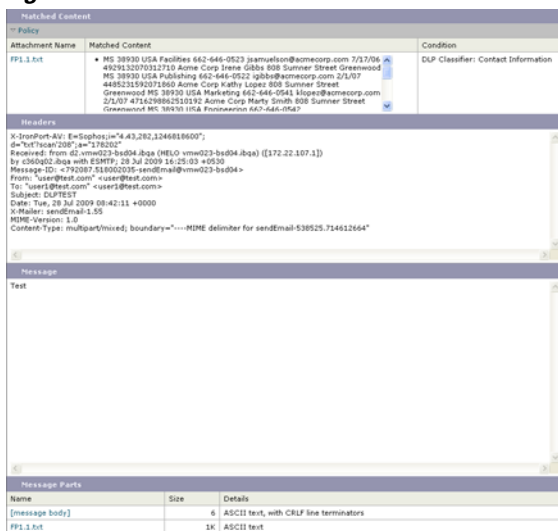
Selecting a Message Action

The three possible actions are to delete the message, release it, or delay the expiration. See for more information.

Step 1   Mark the box corresponding to the message.

Step 2   Select an action from the Select Action menu.

Step 3   Click **Submit**.

> ✎
>
> **Note**   Messages can be placed in multiple quarantines. Please see Multi-User Access and Messages in Multiple Quarantines, page 4-110 for more information about processing messages belonging to multiple quarantines.

Sending a Copy of the Message

Only users belonging to the Administrators group may send copies of a message.

To send a copy of the message, enter an email address in the Send Copy To: field and click **Submit**. Sending a copy of a message does not cause any other action to be performed on the message.

Testing for Viruses

To test the message for viruses, click **Start Test**. Use a quarantine to hold messages until you are sure your anti-virus signatures have been updated.

Testing for viruses sends a copy of the message to the anti-virus engine, not the message itself. The verdict from the anti-virus engine is returned, above the Quarantines area:

Figure 4-9   Scan for Viruses Results

Quarantined Message

Success— AntiVirus scan result was "Clean"

Downloading Attachments

To download an attachment, click the attachment's filename in the Matched Content or Message Parts section. AsyncOS displays a warning that attachments from unknown sources may contain viruses and asks you if you want to continue.

Searching System Quarantines

To search a quarantine for a specific message or messages:

Step 1   Click the name of the quarantine in the Quarantines page. Click **Search Quarantine...** The Search Quarantine page is displayed:

Figure 4-10   Searching Quarantines

Search Quarantine

Search for Quarantined Messages	
Search In:	Policy
For Messages Received:	Last day
Envelope Sender:	Contains
Envelope Recipient(s):	Contains
Subject:	Contains
Display:	20 Per page

Search

Step 2   Enter your search criteria:

–   **Search in**: select a quarantine to search.

–   **For messages received by**: select a time frame.

–   **Envelope Sender**: select "contains," "starts with," "ends with," "matches exactly," or any of the "does not" equivalents, and enter text.

–   **Envelope Recipient(s)**: select "contains," "starts with," "ends with," "matches exactly," or any of the "does not" equivalents, and enter text.

–   **Subject**: select "contains," "starts with," "ends with," "matches exactly," or any of the "does not" equivalents, and enter text.

–   **Display**: select the number of rows to display per page.

✎
Note   The search that is performed is an "AND" search, in that results are returned only if they satisfy all of the criteria specified in the search fields. For example, specifying an Envelope Recipient and a Subject in the search fields, means that only messages that match both the terms specified in Envelope Recipient *and* Subject are returned.

Step 3   Click **Search**.

Step 4   The results (messages that match all of the specified criteria) are displayed.

You can use the search results in the same way you use the quarantine listings. The search results listing also allows sorting by Scheduled Exit time. See Processing Messages in a Quarantine, page 4-102 for more information.

Multi-User Access and System Quarantines

AsyncOS supports delegation of quarantine management by allowing you to specify users from the Operators and Guests groups to process messages within quarantines.

For example:

- the Human Resources team reviews and manages the Policy Quarantine
- the Legal team manages the Confidential Material Quarantine

Operator and Guest users with access to a quarantine can search for messages in that quarantine and process (release and/or delete) messages from that quarantine.

Configuring Multi-User Access

In order to add users to quarantines, the users must already exist. For more information about creating users, see Adding Users, page 8-324.

Each user may have access to all, some, or none of the quarantines. A user that is not authorized to view a quarantine will not see any record of its existence in the GUI or CLI listings of quarantines.

Multi-User Access and Messages in Multiple Quarantines

The policies governing messages that reside in multiple quarantines are "conservative" in that they do not allow a message to be delivered from a quarantine, unless that message has been released from all of the quarantines in which it resides.

When a message is present in multiple quarantines, releasing a message from a quarantine does not necessarily cause that message to be delivered. It must first be released from all of the quarantines in which it resides.

If it has been deleted from any quarantine, the message will still be present in other quarantines. Releasing the message at this point from any other quarantine will not cause the message to be delivered.

Because a message can be in multiple quarantines, and a user wanting to release the message may not have access to all of those quarantines, the following rules apply:

- A message is not released from any quarantine until it has been released from all of the quarantines in which it resides.

- If a message is marked as Deleted in any quarantine, it is not deliverable from any other quarantine in which it resides. It can still be released, but it will not be delivered.

So, if a message is queued in multiple quarantines and a user does not have access to one or more of the other quarantines:

- The user will be informed whether the message is present in each of the quarantines to which the user has access.

- The GUI only shows the scheduled exit time from the quarantines to which the user has access. (For a given message, there is a separate exit time for each quarantine.)

- The GUI will show whether the message is also stored in any other quarantines:

Figure 4-11   Searching Quarantines

- The user will not be told the names of the other quarantine(s) holding the message.

- Releasing a message only affects the queues to which the user has access.

- If the message is also queued in other quarantines not accessible to the user, the message will remain in quarantine, unchanged, until acted upon by users who have the required access to the remaining quarantines (or until it is released "normally" via early or normal expiration).

System Quarantines and Virus Scanning

Once a message has been released for delivery from all queues in which is has been quarantined, it will be rescanned for viruses (assuming anti-virus is enabled on that mail policy) before it can be delivered.

When a message is released from quarantine it is scanned for viruses by the anti-virus engine (if anti-virus is enabled). If the verdict produced (CLEAN, VIRAL, UNSCANNABLE, etc.) matches the verdict produced the previous time the message was processed, the message is not re-quarantined. Conversely, if the verdicts are different, the message could be sent to the Virus quarantine.

The rationale is to prevent messages from looping back to the quarantine indefinitely. For example, suppose a message is encrypted and therefore sent to the Virus quarantine. If an administrator releases the message, the anti-virus engine still will not be able to decrypt it; however, the message should not be re-quarantined or a loop will be created and the message will never be released from the quarantine. Since the two verdicts are the same, the system bypasses the Virus quarantine the second time.

System Quarantines and Alerts

An alert is sent whenever a quarantine reaches or passes 75% and 95% of its capacity. The check is performed when a message is placed in the quarantine. So, if adding a message to the Policy quarantine increases the size to or past 75% of the capacity specified, an alert is sent:

```
Warning: Quarantine "Policy" is 75% full
```

For more information about Alerts, see the "System Administration" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

System Quarantines and Logging

AsyncOS individually logs all messages that are quarantined:

```
Info: MID 482 quarantined to "Policy" (message
filter:policy_violation)
```

The message filter or Virus Outbreak Filters feature rule that caused the message to be quarantined is placed in the parenthesis. A separate log entry is generated for each quarantine in which the message is placed.

AsyncOS also individually logs messages that are removed from quarantine:

```
Info: MID 483 released from quarantine "Policy" (queue full)
```

```
Info: MID 484 deleted from quarantine "Anti-Virus" (expired)
```

The system individually logs messages after they are removed from all quarantines and either permanently deleted or scheduled for delivery, e.g.

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

When a message is re-injected, the system creates a new Message object with a new MID. This is logged using an existing log message with a new MID "byline", e.g.

```
Info: MID 483 rewritten to 513 by System Quarantine
```

The Virus Outbreak Filters Feature and the Outbreak Quarantine

The Outbreak quarantine is present when a valid Virus Outbreak Filters feature license key has been entered. The Virus Outbreak Filters feature sends messages to the Outbreak quarantine, depending on the threshold set. For more information, see the "Virus Outbreak Filters" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

If the license for the Virus Outbreak Filters feature expires, you will be unable to add more messages to the Outbreak quarantine. Once the messages currently in the quarantine have expired and the Outbreak quarantine becomes empty, it is no longer shown in the Quarantines listing in the GUI.

The Outbreak quarantine functions just like other quarantines — you can search for messages, release or delete messages, etc. Messages placed in the Outbreak quarantine are automatically released if newly published rules deem the quarantined message no longer a threat.

The Outbreak quarantine has some additional features, not available in other quarantines: the Manage by Rule Summary link, the Send to IronPort feature when viewing message details, and the option to sort messages in sort results by Scheduled Exit time.

If the appliance has either the IronPort Anti-Spam or Intelligent Multi-Scan feature, the anti-spam scanning engine scans every message released from the Outbreak quarantine based on the mail flow policy that applies to the message.

Manage Rule by Summary Link

Click the Manage by Rule Summary link next to the Outbreak quarantine in the quarantine listing to view the Manage by Rule Summary page. You can perform message actions (Release, Delete, Delay Exit) on all of the messages in the quarantine based on which outbreak rule caused the message to be quarantined. This is ideal for clearing out large amounts of messages from the Outbreak quarantine. For more information, see the "Virus Outbreak Filters" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Send to IronPort

When viewing message details for a message in the Outbreak quarantine, you can optionally report the message to IronPort. Do this to report false positives or to report suspicious messages to IronPort.

To send a copy of a message to IronPort:

Step 1   On the Message Details page, mark the Send a Copy to IronPort Systems box:

Figure 4-12   *Searching Quarantines*

Step 2   Click **Send**. A copy of the message is sent to IronPort Systems.

Configuring the IronPort Spam Quarantines Feature

Each IronPort appliance can have a local IronPort Spam quarantine enabled if the IronPort anti-spam has been enabled. Each IronPort appliance can also refer to an external IronPort Spam quarantine, configured on another IronPort appliance

(typically an M-Series appliance, see "The IronPort M-Series Security Management Appliance" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*for more information).

However, when both the local and an external IronPort Spam quarantine is enabled the *local IronPort Spam quarantine is used*.

Follow these steps to configure your IronPort appliance to send spam or suspect spam messages to an IronPort Spam quarantine (local or external):

Step 1   Add an external IronPort Spam quarantine (see Configuring an External IronPort Spam Quarantine, page 4-127) or enable and configure the local IronPort Spam quarantine (see Configuring the Local IronPort Spam Quarantine, page 4-120). Configuring the local IronPort Spam quarantine allows you to specify settings related to quarantine access, contents, and behavior, notifications, authentication, and AsyncOS user access.

Step 2   If you are configuring the local IronPort Spam quarantine, edit an IP interface and enable the IronPort Spam quarantine HTTP or HTTPS service (see Enabling the IronPort Spam Quarantine HTTP/S Service on an IP Interface, page 4-129). Enabling the IronPort Spam quarantine HTTP/S service allows you to access the quarantine.

Step 3   If you want to migrate from a local IronPort Spam quarantine to an external IronPort Spam Quarantine, configure the anti-spam settings, set a shorter expiration time, and delete all of the remaining messages in the local quarantine. (see Migrating from a Local IronPort Spam Quarantine to an External Quarantine, page 4-117).

Step 4   Configure the anti-spam scanning options for the policy to send spam or suspect spam (or both) to the IronPort Spam Quarantine (see Enabling IronPort Spam Quarantines for a Mail Policy, page 4-131). This step is where you actually configure the system to quarantine spam or suspect spam.

Step 5   See Considerations for Deployment, page 4-132. This important section provides a wealth of additional guidance and information about the IronPort Spam quarantine, including notifications, authentication, and configuration of other related AsyncOS features.

Enabling and Disabling the Local IronPort Spam Quarantine

Enabling the local IronPort Spam quarantine causes AsyncOS to use the local IronPort Spam quarantine, even if you have an external IronPort Spam quarantine configured.

To enable the local IronPort Spam quarantine:

Step 1   On the Monitor > Quarantines page, click Enable.

Figure 4-13   ***Enabling the Local IronPort Spam Quarantine***

Quarantines

Quarantine	Messages	Default Action	Status	Settings
Add Quarantine...				
IronPort Spam Quarantine (disabled)	--	--	--	Enable
Outbreak [Manage by Rule Summary]	0	Retain 12 hours then Release	0% Full	Edit
Policy	1	Retain 10 days then Delete	0% Full	Edit
Virus	0	Retain 30 days then Delete	0% Full	Edit

Step 2   The IronPort Spam Quarantine is enabled. If the IronPort Spam Quarantine is not configured, the Edit IronPort Spam Quarantine page is displayed (see Configuring the Local IronPort Spam Quarantine, page 4-120).

Step 3   Submit and commit your changes.

Disabling the Local IronPort Spam Quarantine

To disable the local IronPort Spam quarantine (not available on the M-Series appliance):

Step 1   On the Monitor > Quarantines page, click Edit in the Settings column for the IronPort Spam Quarantine.

Step 2   In the Spam Quarantine Settings section, uncheck Enable IronPort Spam Quarantine.

Step 3   Submit and commit your changes.

If messages are present in the local IronPort Spam quarantine when it is disabled, you can opt to delete all of the messages via the "Delete All" link on the Quarantines page:

Figure 4-14   The "Delete All" Link on the Quarantines Page

Quarantines

Quarantine	Messages	Default Action	Status	Settings
IronPort Spam Quarantine (disabled)	Delete All	Retain 14 days then Delete	--	Enable
Outbreak [Manage by Rule Summary]	0	Retain 12h then Release	0% Full	Edit
Policy	0	Retain 10d then Delete	0% Full	Edit
Virus	0	Retain 30d then Delete	0% Full	Edit

(Add Quarantine... button above table)

Note   The Delete All link is not available on the IronPort M-Series appliance. To remove all messages from the IronPort Spam quarantine on an M-Series appliance, stop sending spam to it and allow the quarantined messages to expire.

Disabled IronPort Spam Quarantines and Mail Policies

If the IronPort Spam quarantine is disabled, any mail polices set to quarantine spam or suspected spam will instead be set to deliver the message.

Migrating from a Local IronPort Spam Quarantine to an External Quarantine

If you are currently using the local IronPort Spam Quarantine on a local IronPort C- or X-Series appliance but would like to migrate to an external IronPort Spam Quarantine hosted on an IronPort M-series appliance — while retaining access to the messages in the local quarantine — consider the following possible strategies:

- Configuring Anti-Spam Settings — configure the anti-spam settings on your mail policy specifying the M-Series appliance as the alternate host. This action sends new spam to the external quarantine while still allowing access to the local quarantine.

- Setting a shorter expiration time — configure the Schedule Delete After setting on the local quarantine to a shorter duration.

- Delete all of the remaining messages — to delete all of the remaining messages in the local quarantine, disable the quarantine and the click the "Delete All" link on the local quarantines page (see Deleting Messages from the IronPort Spam Quarantine, page 4-142). This link only becomes available when a local IronPort Spam Quarantine with messages still contained in it has been disabled.

You should now be ready to disable the local quarantine and enable the external quarantine while preventing new messages from entering the local quarantine during the transition.

IronPort Spam Quarantine Settings

Spam Quarantine Settings

Set quarantine size, deletion/retention policy, default language, and enable or disable IronPort notification. By default the local IronPort Spam quarantine is self-managing. This means that, once enabled, the quarantine will automatically delete spam after a set amount of time. If the quarantine gets full, older spam is deleted. You can configure and customize the look and behavior of the IronPort Spam quarantine, including specifying a custom logo and login page message. See Configuring Spam Quarantine Settings for the Local IronPort Spam Quarantine, page 4-120.

Specify AsyncOS Operator users that may view or interact with the messages in the local IronPort Spam quarantine. All Administrator level users (such as the default 'admin' user) created in AsyncOS are automatically able to access and modify the IronPort Spam quarantine. Operators can view quarantine contents, but may not change the quarantine settings. See Configuring Administrative Users for IronPort Spam Quarantines, page 4-122.

IronPort Spam Quarantine Access

Allow end users to access and manage their messages in the IronPort Spam quarantine directly via a web browser. Users with access will be able to view, search, release, and delete messages from the quarantine regardless of whether

they have received a spam notification. Specify whether to hide or show message bodies. You can specify the end user authentication used (LDAP, Active Directory, IMAP/POP, or None). See Configuring End User Quarantine Access, page 4-123. Specifying "None" indicates that end users will only be allowed to access the IronPort Spam Quarantine via the links included in notification messages, but they will not be authenticated (does not require a username and password).

Table 4-2   End User Authentication and Access

Authentication	Users Access Via...
LDAP	URL, Notification
Mailbox (IMAP/POP)	URL, Notification
None	Notification Only
Disabled	N/A (If enabled, notifications are sent to the "Deliver Bounce Messages To:" address configured via the Spam Notifications section.)

Spam Notifications

A notification is a digest of new spam messages in the IronPort Spam quarantine for a particular user. Enable and configure the content of the spam notifications, including: the From: address, subject, message body, message format, bounce address, and notification schedule. Notifications allow end users to access their quarantined messages without using LDAP or mailbox authentication, providing IronPort Spam Quarantine access is enabled. Notifications are sent to each Envelope Recipient that has quarantined email, including mailing lists and other aliases. Each mailing list will receive a single digest. This means that all subscribers to a mailing list will receive the notification and can log in to the quarantine to release or delete messages. In this case, users visiting the quarantine to view messages mentioned in a notification may find those messages have already been deleted by other users. Users belonging to multiple aliases and/or using multiple email addresses will receive multiple notifications (see Receiving Multiple Notifications, page 4-136). See Configuring Spam Notifications, page 4-125.

✎

Note   If Spam notifications are enabled, but IronPort Spam Quarantine access is not enabled, notifications will be sent to the "Deliver Bounce Messages To:" address.

Configuring the Local IronPort Spam Quarantine

Once the local IronPort Spam quarantine is enabled (see Enabling and Disabling the Local IronPort Spam Quarantine, page 4-116), you can edit the quarantine's settings to configure the IronPort Spam quarantine and how users will interact with it.

To configure the local IronPort Spam quarantine, click Edit in the Settings column for the IronPort Spam Quarantine on the Monitor > Quarantines page. The Edit IronPort Spam Quarantine page is displayed.

Configuring Spam Quarantine Settings for the Local IronPort Spam Quarantine

To edit the IronPort Spam Quarantine settings for the IronPort Spam quarantine on the local IronPort appliance:

Step 1   Click Edit in the Settings column for the IronPort Spam Quarantine on the Monitor > Quarantines page. The Edit IronPort Spam Quarantine page is displayed.

Figure 4-15   Editing the IronPort Spam Quarantine Settings

Spam Quarantine Settings

☑ Enable IronPort Spam Quarantine

Quarantine Size:	Total: 5 GB ▾ (20.0 GB maximum) ☑ When storage space is full, automatically delete oldest messages first
Schedule Delete After:	◉ 14 days ○ Do not schedule delete
Default Language:	English/United States en-us ▾
Notify IronPort Upon Message Release:	☐ Send a copy of released messages to IronPort for analysis(recommended)
Spam Quarantine Appearance:	Current Logo: (I) **IRONPORT** Spam Quarantine ◉ Use Current Logo ○ Use Ironport Spam Quarantine Logo ○ Upload Custom Logo: [ ] Browse... *Maximum size 500w x 50h pixels* Login Page Message:

Administrative Users

You have no 'operator' users defined in your system.
Go to System Administration > to configure users.
Members of the 'Administrator' group have full access to Quarantines and will automatically be granted access to the
Ironport Spam Quarantine.

Step 2   In the Spam Quarantine Settings section, specify a maximum quarantine size.

Step 3   You can configure the quarantine to delete the oldest messages when the quarantine is full. If unchecked, newer messages will not be added to a full quarantine. IronPort recommends that you enable this feature so that a full quarantine will not cause messages to queue (back up) on your appliance.

Step 4   Specify the number of days to hold messages before deleting them, or you can elect to not schedule automatic deletion. IronPort recommends that you configure the quarantine to delete older messages to prevent the quarantine from filling to capacity.

Step 5   Specify a default language.

Step 6   You can configure the quarantine to send a copy of released messages to IronPort for analysis. IronPort recommends that you do configure the quarantine to do so.

Step 7   Customize the page end users see when they view the quarantine. Upload a custom logo (optional). The logo is displayed at the top of the IronPort Spam quarantine page when the user logs in to view quarantined messages.

—   The logo should be a .jpg, .gif, or .png file that is at most 550 x 50 pixels.

—   If a logo file is not supplied, the default IronPort Spam Quarantine logo is used.

> ✎
>
> **Note**   If you specify a custom logo the IronPort logo is deleted.

Step 8   Specify a login page message. This message is shown to end users when they are asked to log in prior to viewing the quarantine.

Step 9   Submit and commit your changes.
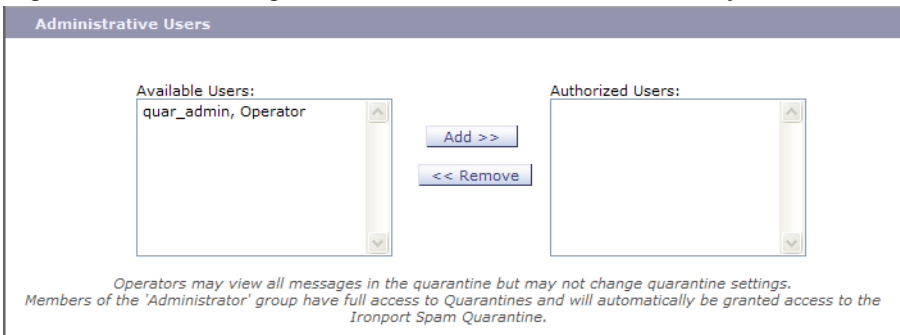
> ✎
>
> **Note**   If you are configuring an IronPort M-Series appliance, see the *Cisco IronPort AsyncOS for Security Management User Guide* for more information.

Configuring Administrative Users for IronPort Spam Quarantines

You can specify administrative users for the IronPort Spam quarantine. In this case, "administrative" refers to the user's access to the IronPort Spam quarantine. Only operator users may be added to the list of administrative users. All administrator level users (including the default admin user) are automatically considered administrative users for the IronPort Spam quarantine, and so they are not listed in the Available or Authorized Users columns.

To add AsyncOS operator users to or remove them from the list of users allowed to view all messages in the IronPort Spam quarantine:

Figure 4-16   Editing Administrative Users for the IronPort Spam Quarantine

Step 1   Select a user in the appropriate list and click **Add** or **Remove**.

Step 2   The user is moved to the opposite list. Note that Operator level users may view messages in the IronPort Spam quarantine, but may not edit the settings of the quarantine. Administrative users can view messages and change the settings.

Step 3   Submit and commit your changes.

Configuring End User Quarantine Access

To allow end users to access the IronPort Spam quarantine directly (without requiring a notification): click Edit in the Settings column for the IronPort Spam Quarantine on the Monitor -> Quarantines page. The Edit IronPort Spam Quarantine page is displayed.

Step 1   Check the checkbox labeled Enable End-User Quarantine Access. Administrator users can still access the quarantine, regardless of whether the box is checked.

Figure 4-17   Editing IronPort Spam Quarantine Access Settings

Step 2   Specify whether or not to display message bodies before messages are released. If this box is checked, users may not view the message body via the IronPort Spam quarantine page. Instead, to view a quarantined message's body users must release the message and view it in their mail application (Outlook, etc.). This is especially relevant to compliance issues where all viewed email must be archived.

Step 3   Specify the method you would like to use to authenticate end-users when they attempt to view their quarantine directly via web browser (not via the email notification). You may use either Mailbox or LDAP authentication.

Note that you can allow end user access to the IronPort Spam quarantine without enabling authentication. In this case, users can access the quarantine via the link included in the notification message and the system does not attempt to authenticate the user. If you want to enable end user access without authentication, select None in the End-User Authentication dropdown menu.

LDAP Authentication: **If you do not have an LDAP server or an active end user authentication query set up, click the System Administration > LDAP link to configure your LDAP server settings and end user authentication query string.** For information about configuring LDAP authentication, see "LDAP Queries" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Mailbox Authentication: For sites without an LDAP directory to use for authentication, the quarantine can also validate user's email addresses and passwords against and standards-based IMAP or POP server that holds their mailbox. When logging in to the web UI, the users enter their full email address and mailbox password, and the quarantine uses this to attempt to log in to the mailbox server as that user. If the login is successful, the user is authenticated and the quarantine then immediately logs out and no changes are made to the user's inbox. Using mailbox authentication works well for sites that do not run an LDAP directory, but mailbox authentication can not present a user with messages that may have been bound for an email alias.

Select the type (IMAP or POP). Specify a server name and whether or not to use SSL for a secure connection. Enter a port number for the server. Supply a domain (example.com, for example) to append to unqualified usernames.

If the POP server advertises APOP support in the banner, then for security reasons (i.e., to avoid sending the password in the clear) the IronPort appliance will only use APOP. If APOP is not supported for some or all users then the POP server should be reconfigured to not advertise APOP.

Step 4   Submit and commit your changes.

Configuring Spam Notifications

Spam notifications are email messages sent to end users when they have messages in the IronPort Spam quarantine. Notifications contain a listing of quarantined spam or suspected spam for the user (or email addresses associated with that user in the LDAP repository, if user authentication is via LDAP, see Configuring End User Quarantine Access, page 4-123). Notifications also include a link for users to use to view their quarantined messages. Once enabled, notifications are sent according to the schedule set here.

Spam notifications provide an alternative method for end-users to log into the quarantine. Users access the quarantine through the email notification they receive (if notifications are enabled for the quarantine). Clicking on any message subject logs the user into the web UI for the quarantine for the email address to which that notification was sent. This method of accessing the IronPort Spam Quarantine does not require LDAP or Mailbox authentication. Note that logging in through this method will not display quarantined messages for any other aliases the end-user may have unless the appliance is using a spam quarantine alias consolidation query for email notifications. If the notification was sent to a distribution list that is expanded after processing by the IronPort appliance, then multiple recipients may have access to the same quarantine for that list.

Because of the way the IronPort appliance generates spam notifications, users may receive multiple spam notifications for their email aliases or if they use multiple email addresses. You can use the alias consolidation feature to prevent some occurrences of multiple notifications. **If you do not have an LDAP server or an active alias consolidation query set up, click the System Administration > LDAP link to configure your LDAP server settings and alias consolidation query string.** For more information, see "LDAP Queries" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*, as well as Considerations for Deployment, page 4-132 and Receiving Multiple Notifications, page 4-136 in this guide.

To configure spam notifications sent to end users:

Step 1   Enable spam notifications by checking the checkbox labeled Enable Spam Notifications.

Figure 4-18   Configuring Spam Notifications

Step 2   Enter a From: address for the notifications. Users may want to add this address to any "whitelist" supported by their email client (see Considerations for Deployment, page 4-132).

Step 3   Enter a subject for the notification.

Step 4   Enter a customized title for the notification.

Step 5   Customize the message body. AsyncOS supports several message variables that, when placed in the message body, are expanded to the actual value for the specific end user. For example, %username% is expanded to the actual user's name when the notification is generated for that user. The supported message variables include:

–   **New Message Count** (%new_message_count%) - the number of new messages since the user's last login.

–   **Total Message Count** (%total_message_count%) - the number of messages for the user in the end user quarantine.

–   **Days Until Message Expires** (%days_until_expire%)

– **Quarantine URL** (`%quarantine_url%`) - URL to log in to quarantine and view messages.

– **Username** (`%username%`)

– **New Message Table** (`%new_quarantine_messages%`) - A listing of new messages in the quarantine for the user.

You can include these message variables in the message body by typing them directly in the text of the Message Body field, or you can place the cursor where you would like the variable inserted and then click on the name of the variable in the Message Variables listing on the right.

Step 6   Select a message format (HTML, Text, or HTML/Text).

Step 7   Specify a bounce address (bounced notifications will be sent to this address).

Step 8   Optionally, you can consolidate messages sent to the same LDAP user at different addresses.

Step 9   Set the notification schedule. You can configure the notifications to be sent once a month, once a week, or one or more times a day (with or without weekends).

Step 10   Submit and commit your changes.

Configuring an External IronPort Spam Quarantine

You can configure your IronPort appliance to send spam and suspect spam to an external IronPort Spam quarantine configured on a separate IronPort appliance. The IronPort M-Series appliance is specifically designed to perform this role. For more information about the IronPort M-Series appliance, see "The IronPort M-Series Security Management Appliance" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

If you use an external IronPort Spam quarantine, the quarantine settings are configured on that IronPort appliance. If you have both the local and an external IronPort Spam quarantine enabled on your IronPort appliance, the local IronPort Spam quarantine, along with its settings, take precedence.

Messages that are released from the M-Series appliance (external quarantine) will skip the RAT, domain exceptions, aliasing, incoming filters, masquerading, bounce verification, and the work queue.

Adding an External IronPort Spam Quarantine

To add an external IronPort Spam quarantine:

Step 1   From the Monitor > External Spam Quarantine page, click **Add Quarantine...**
The External Quarantines page is displayed.

Figure 4-19   Adding an External End User Quarantine

External Quarantines

External Quarantines
Add Quarantine...
No external quarantines defined.

Step 2   Enter a name for the quarantine. The name is not significant, and is used for reference only.

Step 3   Enter an IP address and port number. The IP Address and port number are specified on the M-Series appliance in the Spam Quarantines Settings page (for more information, see the *Cisco IronPort AsyncOS for Security Management User Guide*).

Step 4   Submit and commit your changes.

Editing an External IronPort Spam Quarantine

To edit an existing external IronPort Spam quarantine:

Step 1   Click Edit in the Settings column. The Edit External Quarantine page is displayed.

Step 2   Make changes to the settings.

Step 3   Submit and commit changes.

Removing an External IronPort Spam Quarantine

You can only have one external IronPort Spam quarantine specified on your IronPort appliance. Please note that removing an external IronPort Spam quarantine does not mean that the quarantine itself is deleted or that the data within the quarantine is changed in any way. Instead, the reference to that external IronPort Spam quarantine is removed from the local machine.

To remove an external IronPort Spam quarantine:

Step 1   Click Edit in the Settings column. The Edit External Quarantine Page is displayed.

Step 2   Click Remove Settings.

Figure 4-20   Removing an External IronPort Spam Quarantine

Edit External Quarantine

Step 3   You are prompted to click **Delete** to confirm the deletion.

Enabling the IronPort Spam Quarantine HTTP/S Service on an IP Interface

Once you have enabled the local IronPort Spam quarantine, enable the IronPort Spam quarantine HTTP or HTTPS service on an IP interface.

To enable the IronPort Spam quarantine HTTP or HTTPS service on an IP interface:

Step 1   On the Network > IP Interfaces page, click on the interface name (for this example, we will use the Management interface). The Edit IP Interface dialog is displayed:

Figure 4-21   Enabling the IronPort Spam Quarantine on the Management Interface

Step 2   Specify whether to use HTTP or HTTPS as well as the associated port numbers.

Step 3   Select whether to redirect HTTP requests to HTTPS.

Step 4   Specify whether this is the default interface (notifications and quarantine logins will originate on this interface) for IronPort Spam quarantine access. Select whether to use the hostname in the URL or specify a custom URL.

Step 5   Submit and commit your changes.

Enabling IronPort Spam Quarantines for a Mail Policy

Once you have enabled the local IronPort Spam quarantine (or added an external IronPort Spam quarantine) you can configure a mail policy to send spam or suspected spam messages to that quarantine. Note that you must have IronPort Anti-Spam scanning enabled on the mail policy in order to be able to send mail to the IronPort Spam quarantine.

To configure a mail policy to send spam or suspect spam to the IronPort Spam Quarantine:

Step 1   On the Mail Policies > Incoming Mail Policies page, click the link in the Anti-Spam column for the corresponding mail policy.

Figure 4-22   ***Modifying a Mail Policy to Send Spam to the IronPort Spam Quarantine***

Step 2   The Mail Policies: Anti-Spam page is displayed.

Step 3   In the Positively-Identified Spam Settings section, select IronPort Spam Quarantine for the Apply This Action to Message option.

Figure 4-23   ***Sending Positively Identified Spam to the IronPort Spam Quarantine***

Step 4   Repeat this for Suspected spam if desired.

Step 5   Submit and commit your changes.

Considerations for Deployment

This section consists of various tips and information to keep in mind when deploying the IronPort Spam quarantine.

Disk Space

Table 4-3 shows the amount of disk space available on each appliance for the IronPort Spam Quarantine.

Table 4-3   Disk Space Available for IronPort Spam Quarantine by IronPort Appliance

Model	Disk Space (in GBytes)
C10/100/150/160	5
C30	10
C300/350/360	15
C60	20
C600/650/660/X1000/1050/1060	30
M600/650/660	100
M1000/1050/1060	200

End Users Accessing the IronPort Spam Quarantine

End users can access the IronPort Spam quarantine via a link in the notification they receive. When accessing the quarantine via this method, LDAP or IMAP/POP authentication is not required (end users do not have to authenticate themselves). Note that the links present in the notification messages do not expire, so end users can use these links to view their quarantined messages without having to authenticate.

Users can also access the quarantine by entering a link in their web browser directly. When accessing the quarantine via a URL typed into a web browser, users will have to authenticate. The authentication method — LDAP or "mailbox" (IMAP/POP) — is defined in the End User Quarantine Access section of the quarantine settings (see Configuring End User Quarantine Access, page 4-123).

LDAP Authentication

The authentication process for LDAP works like this:

Step 1   A user enters their username and password into the web UI login page.

Step 2 The IronPort Spam quarantine connects to the specified LDAP server either to perform an anonymous search or as an authenticated user with the specified "Server Login" DN and password. For Active Directory, you will usually need to have the server connect on the "Global Catalog port" (it is in the 6000s) and you need to create a low privilege LDAP user that the IronPort Spam quarantine can bind as in order to execute the search.

Step 3 The IronPort Spam quarantine then searches for the user using the specified BaseDN and Query String. When a user's LDAP record is found, the IronPort Spam quarantine then extracts the DN for that record and attempts bind to the directory using the user records' DN and the password they entered originally. If this password check succeeds then the user is properly authenticated, but the IronPort Spam quarantine still needs to determine which mailboxes' contents to show for that user.

Step 4 Messages are stored in the IronPort Spam quarantine using the recipient's envelope address. After a user's password is validated against LDAP, the IronPort Spam quarantine then retrieves the "Primary Email Attribute" from the LDAP record to determine which envelope address they should show quarantined messages for. The "Primary Email Attribute" can contain multiple email addresses which are then used to determine what envelope addresses should be displayed from the quarantine for the authenticated user.

IMAP/POP Authentication

The authentication process for IMAP/POP works like this:

Step 1 Depending on your mail server configuration, a user enters their username (`joe`) or email address (`joe@example.com`) and password into the web UI login page. You can modify the Login Page Message to tell your users whether they should enter a full email address or just their username (see Configuring End User Quarantine Access, page 4-123).

Step 2 The IronPort Spam quarantine connects to the IMAP or POP server and uses the entered login (either username or email address) and password to try to log into the IMAP/POP server. If the password is accepted then the user is considered authenticated and the IronPort Spam quarantine immediately logs out of the IMAP/POP server.

Step 3 Once the user is authenticated, the IronPort Spam Quarantine lists email for the user, based on the email address:

- If you have configured the IronPort Spam quarantine to specify a domain to append to bare usernames (like `joe`), then this domain is appended and that fully qualified email address is used to search for matching envelopes in the quarantine.

- Otherwise, the IronPort Spam quarantine uses the entered email address to search for matching envelopes.

Determining the URL for Logging in to the IronPort Spam Quarantine

The URL end users can use to access the IronPort Spam quarantine directly is formed from the hostname of the machine and the settings (HTTP/S and port numbers) configured on the IP interface on which the quarantine has been enabled. For example,

```
HTTP://mail3.example.com:82
```

Example Configurations

Example POP/IMAP Configurations:

On IMAP and POP (single domain):

- Enter the server name.
- Enable SSL if you have configured your server to use it.
- Enable "Append Domain to Unqualified Usernames" and set this to the domain of the envelope for users logging in.

For more information about IMAP, see the University of Washington website:

```
http://www.washington.edu/imap/
```

Testing Notifications

You can test notifications by configuring a testing mail policy in the Email Security Manager, and have spam quarantined for just a single user. Then, configure the IronPort Spam Quarantine notification settings: check the "Enable Spam Notification" checkbox and do not check "Enable End-User Quarantine Access" checkbox. Then only the administrator configured in the "Deliver Bounced Messages To" field is notified of new spam in the quarantine.

Ensuring that End Users Receive the Notifications

Consider recommending that end users add the From: address for the IronPort Spam Quarantine notification emails to the "whitelist" in their Mail application's (Outlook, Thunderbird, etc.) Junk Mail Settings.

Receiving Multiple Notifications

Users belonging to multiple email aliases or using several email addresses will receive multiple notifications. This is also the case for users belonging to LDAP groups receiving email.

Table 4-4   Notifications per Address/Alias

User	Email Addresses	Aliases	Notifications
Sam	sam@example.com		1
Mary	mary@example.com	dev@example.com, qa@example.com, pm@example.com	4
Joe	joe@example.com, admin@example.com	hr@example.com	3

Note   If you do not use LDAP and you do not want your end users to receive multiple email notifications, consider disabling notifications and instead allow end users to access the quarantine directly and authenticate via LDAP or POP/IMAP.

Determining Which Messages are Present for Each User

Depending on the method of authentication (LDAP or IMAP/POP) users may see mail for multiple email address in the IronPort Spam quarantine.

When using LDAP authentication, if the Primary Email attribute has multiple values in the LDAP directory, all of those values (addresses) will be associated with the user. Therefore, quarantined messages addressed to all email addresses associated with the end user in the LDAP directory are present in the quarantine.

If, however, the user accesses the quarantine directly via a notification, or if the authentication method is IMAP/POP, the quarantine will only display messages for that user's email address (or the address to which the notification was sent). For more information about how end user authentication works, see End Users Accessing the IronPort Spam Quarantine, page 4-133.

Keep in mind that email addresses are case insensitive in the IronPort Spam Quarantine, so for example, email for Admin@example.com and admin@example.com will both be present in the quarantine for a user associated with "admin@example.com."

Limiting which Addresses have Mail Quarantined

You can use multiple mail policies (Mail Policies > Incoming Mail Policy) to specify a list of recipient addresses for which mail will not be quarantined. Select 'Deliver' or 'Drop' instead of quarantine when configuring the anti-spam settings for the mail policy.

Default Encoding

AsyncOS attempts to determine the charset of a message based on the encoding specified in the message headers. However, if the encoding specified in the headers does not match that of the actual text, the message will not be displayed properly when viewed in the IronPort Spam quarantine. This situation is more likely to occur with spam messages.

Specifying a Default Encoding

In the case where incoming email does not have a charset encoding specified in the headers, you can configure your IronPort appliance to specify a default encoding. Doing so will help ensure that these types of messages display properly in the IronPort Spam quarantine.

However, specifying a default encoding can cause messages in other charsets to display incorrectly. This applies only to messages that do not specify the encoding in the message headers. Generally, you would only want to set a default encoding if you expect the majority of your mail that falls into this category to be of one specific encoding. For example, if the majority of your mail that gets quarantined and that does not specify the charset encoding in the message headers is in Japanese (ISO-2022-JP), you would select option 12 (in the `scanconfig->setup`

options, below) when prompted: `Configure encoding to use when none is specified for plain body text or anything with MIME type plain/text or plain/html.`

To set a default encoding for messages that do not specify the encoding in the message headers, use the `scanconfig->setup` command via the CLI. In this example, UTF-8 is set as the default:

```
mail3.example.com> scanconfig



There are currently 7 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.

[]> setup



[ ... ]

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)

[ ... list of encodings ... ]

13. Japanese (EUC)

[1]> 2



Encoding set to "Unicode (UTF-8)".
```

Managing Messages in IronPort Spam Quarantines

This section explains how to work with messages within local or external IronPort Spam quarantines, from the administrator's point of view. When an administrator views the quarantine, all of the messages contained in the quarantine are available.

As an administrator, you can perform the following actions on messages within the IronPort Spam quarantine:

- View messages
- Deliver messages
- Delete messages
- Search messages

Figure 4-24   IronPort Spam Quarantine Search Page

Searching for Messages in the IronPort Spam Quarantine

Use the search form to search through all of the messages in the IronPort Spam quarantine.

Step 1   Specify an envelope recipient, you can enter a partial address. Select whether the search results should match the exact recipient you entered, or whether the results should contain, start with, or end with your entry.

Step 2   Enter a date range to search through. Click the calendar icons to select a date.

Step 3   Specify a From: address, and select whether the search results should contain, match exactly, start with, or end with the value you entered.

Step 4   Click **Search**. Messages matching your search criteria are displayed below the Search section of the page.

Searching Very Large Message Collections

If you have a very large collection of messages in the IronPort Spam Quarantine, and if your search terms are not narrowly defined, your query may take a very long time to return information, or it may time out.

You will be prompted to confirm whether you want to resubmit your search. Please note that having multiple large searches running simultaneously can impact performance on your IronPort appliance.

Viewing Messages in the IronPort Spam Quarantine

The message listing shows messages in the IronPort Spam quarantine. You can select how many messages are shown at one time. You can sort the display by clicking on the column headings. Click the same column again to reverse the sorting.

Click the subject of a message to view the message, including the body and headers. The message is displayed in the Message Details page. The first 20K of the message is displayed. If the message is longer, it is truncated at 20K and you can download the message via the link at the bottom of the message.

From the Message Details page you can delete a message (select **Delete**) or select **Release** to release the message. Releasing a message causes it to be delivered.

Viewing Messages with Attachments

When viewing a message that includes an attachment, the body of the message is displayed, followed by a list of attachments.

Viewing HTML Messages

The IronPort Spam Quarantine attempts to render an approximation of HTML based messages. Images are not displayed.

Viewing Encoded Messages

Base64 encoded messages are decoded and then displayed.

Delivering Messages in the IronPort Spam Quarantine

To release a message for delivery, click the checkbox next to the message or messages you want to release and select **Release** from the drop-down menu. Then click **Submit**.

Click the checkbox in the heading row to automatically select all of the messages currently displayed on the page.

Released messages proceed directly to the destination queue, skipping any further work queue processing in the email pipeline.

Deleting Messages from the IronPort Spam Quarantine

The IronPort Spam quarantine can be configured to automatically delete messages after a certain amount of time. Also, the IronPort Spam quarantine can be configured to automatically delete the oldest messages once the quarantine has reached its maximum size. You may also delete messages from the IronPort Spam quarantine manually.

To delete specific messages, click the checkbox next to the messages you want to delete and then select **Delete** from the drop-down menu. Then click **Submit**. Click the checkbox in the heading row to automatically select all of the messages currently displayed on the page.

To delete all of the messages in the IronPort Spam quarantine, disable the quarantine (see Disabling the Local IronPort Spam Quarantine, page 4-116) and then click the Delete All Messages link. The number in parenthesis at the end of the link is the number of messages in the IronPort Spam quarantine.

Figure 4-25   Delete All Messages Link

Quarantines				
Add Quarantine...				
Quarantine	Messages	Default Action	Status	Settings
IronPort Spam Quarantine (disabled)	Delete All	Retain 14 days then Delete	--	Enable

Working with Safelists and Blocklists

You can enable end users to create safelists and blocklists to better control which emails are treated as spam. Safelists allow a user to ensure that certain users or domains are never treated as spam, while blocklists ensure that certain users or domains are always treated as spam. The safelists and blocklists settings are configured from the IronPort Spam Quarantine, so you *must* enable and configure the IronPort Spam Quarantine to use this feature. When you enable the safelist/blocklist feature, each end user can maintain a safelist and blocklist for his or her email account.

✎
Note   Safelists and blocklists prevent mail from being treated as spam or ensure that mail is treated as spam. However, a safelist or blocklist setting does not prevent the IronPort appliance from scanning an email for viruses or determining if the

message meets the criteria for a content-related mail policy. If a message is part of a safelist, it may not be delivered to the end user depending on other scanning settings.

The Safelist/Blocklist Database

When a user adds an entry to a safelist or blocklist, the entry is stored in a database on the IronPort appliance. If you use M-series, the database is saved on the M-series appliance and periodically updated and synchronized on all related C-Series appliances. If the IronPort Spam Quarantine is hosted on a C-series appliance, the safelist/blocklist database is maintained on that C-Series appliance. If you use multiple C-Series appliances without an M-Series appliance, you may need to synchronize databases and configuration settings manually. For information about synchronizing safelist/blocklist settings and databases across different C-Series appliances, see Synchronizing Safelist and Blocklist Settings and Databases, page 4-147.

For information about working with the backup .CSV database, see Backing Up and Restoring the Safelist/Blocklist Database, page 4-146.

For more information about working with safelists and blocklists on an M-Series appliance, see the *Cisco IronPort AsyncOS for Security Management User Guide* .

Creating and Maintaining Safelists and Blocklists

The safelists and blocklists are created and maintained by end users. However, an administrator enables the feature and configures delivery settings for email messages matching entries in the blocklist. To create and maintain safelists and blocklists, the administrators and end-users complete the following tasks:

- **Administrator tasks**. Administrators enable and configure the IronPort Spam Quarantine, enable the Safelist/Blocklist feature, backup and restore the Safelist/Blocklist database, synchronize the Safelist/Blocklist database between different appliances, and troubleshoot safelist and blocklist issues via logs, alerts, and custom headers. For more information about administrator tasks, see Administrator Tasks for Creating and Maintaining Safelists and Blocklists, page 4-145.

- **End-user tasks**. End-users create their safelist and blocklist settings via the end-user spam quarantine. End users may need to log in (instead of clicking the link in the IronPort Spam Quarantine notification) to access their safelist/blocklist settings. From the end-user spam quarantine, end-users can create safelists and blocklists from the Options menu. Or, end-users can create safelist settings from the list of quarantined emails. For details about end-user tasks, see End User Tasks for Configuring Safelists and Blocklists, page 4-148.

Message Delivery For Safelists and Blocklists

When you enable safelists and blocklists, the IronPort appliance scans the messages against the safelist/blocklist database immediately prior to anti-spam scanning. If the IronPort appliance detects a sender or domain that matches an end user's safelist/blocklist setting, the message will be splintered if there are multiple recipients (and the recipients have different safelist/blocklist settings). For example, a message is sent to both recipient A and recipient B. Recipient A has safelisted the sender, whereas recipient B does not have an entry for the sender in either safelist or blocklist. In this case, the message may be split into two messages with two message IDs. The message sent to recipient A is marked as safelisted with an *X-SLBL-Result-Safelist* header, and skips anti-spam scanning, whereas the message bound for recipient B is scanned with the anti-spam scanning engine. Both messages then continue along the pipeline (through anti-virus scanning, content policies, etc.), and are subject to any settings configured.

If a message sender or domain is blocklisted, the delivery behavior depends on the blocklist action settings. Similar to safelist delivery, the message is splintered if there are different recipients with different safelist/blocklist settings. The blocklisted message splinter is then quarantined or dropped, depending on the blocklist action settings. If the blocklist action is configured for quarantine, the message is scanned and eventually quarantined. If the blocklist action is configured as drop, the message is dropped immediately after safelist/blocklist scanning.

Because the safelist and blocklists are maintained in the IronPort Spam Quarantine, delivery behavior is also contingent on other anti-spam settings. For example, if you configure the "Accept" mail flow policy in the HAT to skip anti-spam scanning, then users who receive mail on that listener will not have their safelist and blocklist settings applied to mail received on that listener.

Similarly, if you create a mailflow policy that skips anti-spam scanning for certain message recipients, these recipients will not have their safelist and blocklist settings applied.

Administrator Tasks for Creating and Maintaining Safelists and Blocklists

To use safelists and blocklists, the administrator must complete the following tasks:

- **Enable and configure the Ironport Spam Quarantine**. Because the safelist and blocklist is accessed from the IronPort Spam Quarantine, you must enable this feature to use safelists and blocklists. For information, see Configuring the IronPort Spam Quarantines Feature, page 4-114.

- **Enable and configure the Safelist/Blocklist feature**. Once the IronPort Spam Quarantine is enabled, you enable and configure the Safelist/Blocklist feature. You must also configure a blocklist action for blocklisted email (quarantine or delete). For information, see Enabling and Configuring Safelist/Blocklist Settings, page 4-145

- **Backup and restore the Safelist/Blocklist database**. When upgrading, you need to backup and restore the Safelist/Blocklist database. For information, see Backing Up and Restoring the Safelist/Blocklist Database, page 4-146.

- **Synchronize Safelist/Blocklist databases**. When end users enter safelist or blocklist entries, the settings are saved to a database which is periodically synchronized with a database that is used by AsyncOS when processing email. If the IronPort Spam Quarantine is maintained on an M-Series appliance, the administrator must configure the Safelist/Blocklist database to synchronize with the C-Series appliance. For information, see Synchronizing Safelist and Blocklist Settings and Databases, page 4-147.

- **Troubleshooting Safelists and Blocklists**. To troubleshoot safelists and blocklists, you can check logs, alerts. For more information, see Troubleshooting Safelists and Blocklists, page 4-148.

Enabling and Configuring Safelist/Blocklist Settings

You can enable and configure settings for safelists and blocklists from the Quarantines page.

Step 1   To enable safelists and blocklists on a C-Series appliance, go to Monitor >
Quarantines.

> ✎
>
> **Note**   You must have the IronPort Spam Quarantine enabled and configured
> before you can configure safelists and blocklists.

Step 2   In the End-User Safelist/Blocklist settings, select **Edit Settings**.

End-User Safelist/Blocklist (IronPort Spam Quarantine)		
Safelist/Blocklist Settings		
End-User Safelist/Blocklist:	Enabled	
Blocklist Action:	Quarantine	
		Edit Settings...

Step 3   Select Enable Safelist/Blocklist Feature.

Step 4   Select **Quarantine** or **Delete** for the Blocklist Action.

Step 5   Specify the Maximum List Items Per User. This value represents the maximum
number of addresses or domains a user can list in each safe and block list.

Step 6   Click **Submit**.

Backing Up and Restoring the Safelist/Blocklist Database

To save a backup of the safelist/blocklist database, the IronPort appliance saves
the database as a .CSV file. The .CSV file is maintained separately from the XML
configuration file that contains your IronPort appliance configuration settings. If
you upgrade your IronPort appliance or run the Installation Wizard, you should
back up the Safelist/Blocklist database to the .CSV file.

When you back up a file, the IronPort appliance saves a .CSV file to the
/configuration directory using the following naming convention:

slbl<timestamp><serial number>.csv

From the GUI, you can use the following method to back up and restore the
database:

Step 1   From System Administration > Configuration File, go to the End-User Safelist/Blocklist Database section.

End-User Safelist/Blocklist Database (IronPort Spam Quarantine)		
Backup and Restore Database		
Backup:	Filename: slbl-001143EBE31F-1RJGP61-<timestamp>.csv	Backup Now
Restore:	Select File to Restore...	

Step 2   To back up a database to a .CSV files, click **Backup Now**.

Step 3   To restore the database, click **Select File to Restore**.

The IronPort appliance displays a list of backup files that are stored in your configuration directory.

Step 4   Select the safelist/blocklist backup file you want to restore and click **Restore**.

Synchronizing Safelist and Blocklist Settings and Databases

When an end user creates a safelist or blocklist, the setting is saved to a database. If the IronPort Spam Quarantine exists on an M-Series appliance, this database must be synchronized with a database on the C-Series appliance before the safelist/blocklist settings are applied to incoming mail. When the IronPort Spam Quarantine exists on a C-Series appliance, the database must be synchronized with a read-only database that is used when processing the mail queue. The amount of time it takes to automatically synchronize these databases depends on the model of the appliance. The following table shows the default settings for updating safelists and blocklists:

Table 4-5   Synchronization for Safelist and Blocklist Settings

Appliance	Synchronization Time
C10/C100/C150/C160	10 minutes
C30/C300/C350/C360	15 minutes
C60/C600/C650/C660	30 minutes
X1000/X1050/X1060	60 minutes
M600/M660	120 minutes
M1000/M1050/M1060	240 minutes

When you use a group of C-Series appliances without an M-Series appliance, you may need to synchronize the safelist/blocklist settings and database across machines.

If you use the centralized management feature to configure multiple IronPort appliances, you can configure administrator settings using centralized management. If you do not use centralized management, you can manually verify that settings are consistent across machines.

For more information about accessing the appliance using FTP see "Accessing the Appliance" in either the *Cisco IronPort AsyncOS for Email Configuration Guide* or the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Troubleshooting Safelists and Blocklists

An end user maintains his or her own safelists and blocklists. Administrators can access an end user's safelist or blocklist only by logging into the end user account with the user's login and password. To troubleshoot issues with safelists and blocklists, you can view the log files or system alerts.

When an email is blocked due to safelist/blocklist settings, the action is logged in the ISQ_logs or the antispam log files. Emails that are safelisted are marked as safelisted with an *X-SLBL-Result-Safelist* header. Emails that are blocklisted are marked as blocklisted with an *X-SLBL-Result-Blocklist* header.

Alerts are sent out when the database is created, updated, or if there are errors in modifying the database or running the safelist/blocklist processes.

For more information about alerts, see "System Administration" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

For more information about log files, see Chapter 5, "Logging."

End User Tasks for Configuring Safelists and Blocklists

End users can create safelists to ensure that messages from certain senders are never treated as spam, and they can use blocklists to ensure that messages from certain senders are always treated as spam. For example, an end user may receive email from a mailing list that no longer interests him. He may decide to add this sender to his blocklist to prevent emails from the mailing list from getting sent to his inbox. On the other hand, end users may find that emails from specific senders

get sent to their IronPort Spam Quarantine when they don't want them to be treated as spam. To ensure mail from these senders are not quarantined, they may want to add the senders to their safelists.

Note   Safelist/Blocklist settings are contingent on other settings configured by the system administrator.

To work with safelists and blocklists, end users must complete the following tasks:

- **Access safelists and blocklists**. Depending on authentication settings, end users may need to log into their IronPort Spam Quarantine accounts. For more information, see Accessing Safelists and Blocklists, page 4-149.

- **Add safelist entries**. Users add safelist entries from the Options menu or the list of quarantined messages in IronPort Spam Quarantine. For more information, see Adding Entries to Safelists, page 4-150.

- **Add blocklist entries**. Users add blocklist entries from the Options menu of the IronPort Spam Quarantine. For more information, see Adding Entries to Blocklists, page 4-153.

Accessing Safelists and Blocklists

To access safelists and blocklists, end users whose accounts are authenticated using LDAP or Mailbox (IMAP/POP) authentication must log into their accounts on the IronPort Spam Quarantine. The end user must log into their account even if they are accustomed to accessing their messages via a spam notification (which usually doesn't require authentication). If the end-user authentication is set to NONE, end users do not need to log into their accounts to access safelist/blocklist settings.

Syntax for Safelists and Blocklist Entries

Entries can be added to safelists and blocklists using the following formats:

- user@domain.com
- server.domain.com
- domain.com

End users cannot add a sender or domain to both safe and block lists at the same time. However, if the end user adds a domain to a safelist, and the email address for a user of that domain to the blocklist (or vice versa), the IronPort appliance applies both rules. For example, if the end user adds *example.com* to the safelist, and adds *george@example.com* to the blocklist, the IronPort appliance delivers all mail from example.com without scanning for spam, but will treat mail from *george@example.com* as spam.

End users cannot allow or block a range of sub-domains using the following syntax: *.domain.com*. However, an end user can explicitly block a specific domain using the following syntax: *server.domain.com*.

Adding Entries to Safelists

End users can add senders to safelists in two ways:

Method 1

Step 1   From the IronPort Spam Quarantine, select the Options drop-down menu.

Figure 4-26   Safelist Options in the End-User Quarantine
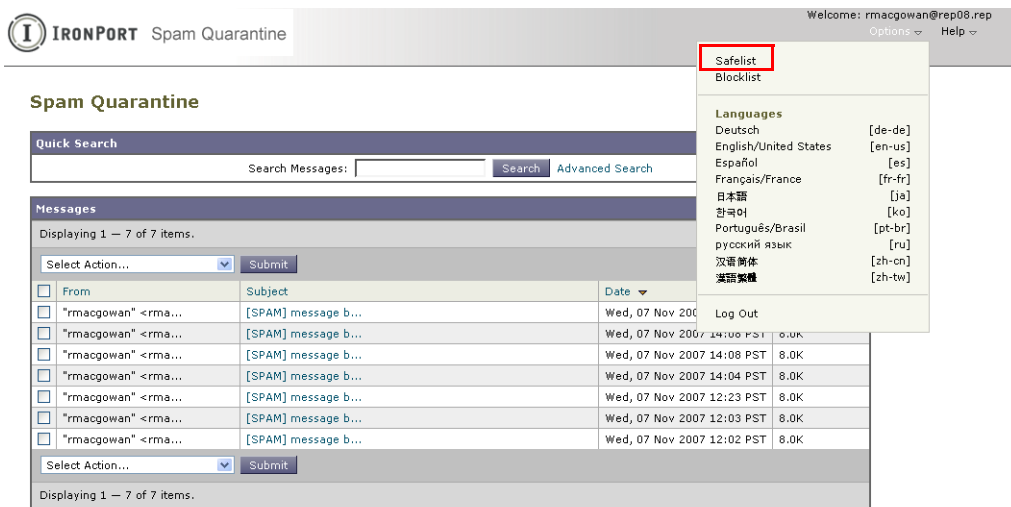
Step 2   Choose Safelist.

Step 3   From the Safelist dialog box, enter the email address or domain. You can enter multiple domains and email addresses, separated by commas.

Step 4   Click **Add to List**.

Figure 4-27   Safelist in End-User Quarantine

Method 2

End users can also add senders to the safelist if the message has been sent to the end user quarantine.

Step 1   From the End-User Quarantine, select the checkbox next to message.

Step 2   Choose "Release and Add to Safelist" from the drop-down menu.

Figure 4-28   Safelist in End-User Quarantine
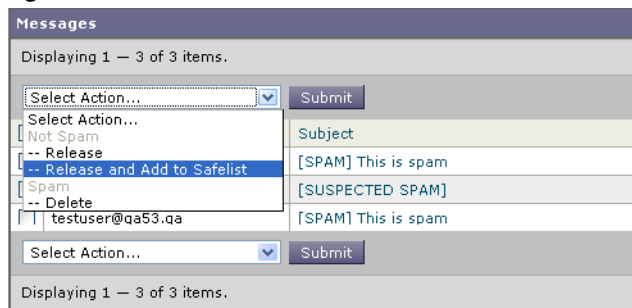
The envelope sender and the from header for the specified mail are both added to the safelist, and the released messages proceed directly to the destination queue, skipping any further work queue processing in the email pipeline.

Adding Entries to Blocklists

End users can use blocklists to ensure that they never receive mail from specified senders.

Step 1   From the End-User Quarantine, select the Options drop-down menu.

Figure 4-29   Blocklist Options in the End-User Quarantine
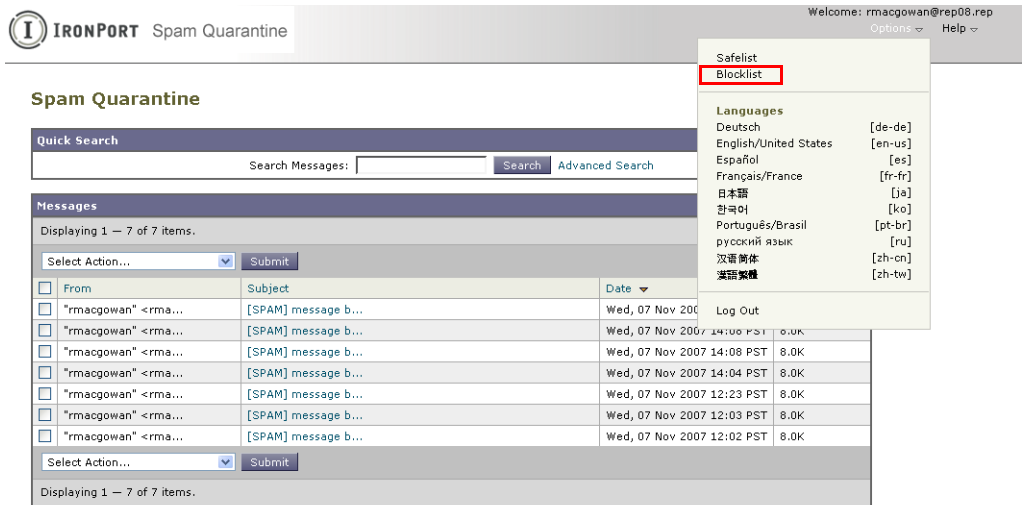
Step 2   Enter the domain or email address you want to blocklist. You can enter multiple domains and email addresses, separated by commas.

Step 3   Click **Add to List**.

Figure 4-30   Adding Senders to a Blocklist

When the IronPort appliance receives mail from the specified email address or domain that matches an entry in the blocklist, it treats the mail as spam. The mail may be rejected or it may be quarantined, depending on the safelist/blockist action settings.

Note   Unlike safelist entries, you can only add blocklist entries from the Options menu in the End-User Quarantine.

C H A P T E R 5

Logging

An important feature of the Cisco IronPort Email Security appliance is its logging capabilities. AsyncOS can generate many types of logs, recording varying types of information. Log files contain the records of regular activity and errors from various components of the system. This information can be valuable when monitoring your Cisco IronPort appliance as well as when troubleshooting or checking performance.

This chapter contains the following sections:

Overview

This section contains the following topics:

Understanding Log Files and Log Subscriptions

Logs are a compact, efficient method of gathering critical information about the email operations of AsyncOS. These logs record information regarding activity on your IronPort appliance. The information will vary depending upon the log you view, for example, Bounce logs or Delivery logs.

Most logs are recorded in plain text (ASCII) format; however, delivery logs are formatted in binary for resource efficiency. The ASCII text information is readable in any text editor.

IronPort offers an off-box centralized reporting and tracking tool for logs from multiple IronPort appliances. See your IronPort representative for more information.

A log subscription associates a log type with a name, logging level, and other constraints such as size and destination information; multiple subscriptions for the same log type are permitted. T

Log Types

The log type indicates what information will be recorded within the generated log such as message data, system statistics, binary or textual data. You select the log type when creating a log subscription. See Log Subscriptions, page 5-206 for more information.

IronPort AsyncOS for Email generates the following log types:

Table 5-1   *Log Types*

Log	Description
IronPort Text Mail Logs	Text mail logs record information regarding the operations of the email system. For example, message receiving, message delivery attempts, open and closed connections, bounces, TLS connections, and others.
qmail Format Mail Logs	qmail format delivery logs record the same information regarding the operations of the email system as delivery logs following, but stored in qmail format.

Table 5-1   Log Types (continued)

Log	Description
Delivery Logs	Delivery logs record critical information about the email delivery operations of the IronPort appliance — for example, information regarding each recipient delivery and bounce at the time of the delivery attempt. The log messages are "stateless," meaning that all associated information is recorded in each log message and users need not reference previous log messages for information about the current delivery attempt. Delivery logs are recorded in a binary format for resource efficiency. Delivery Log files must be post-processed using a provided utility to convert them to XML or CSV (comma-separated values) format. The conversion tools are located at: `http://support.ironport.com`
Bounce Logs	Bounce logs record information about bounced recipients. The information recorded for each bounced recipient includes: the message ID, the recipient ID, the Envelope From address, the Envelope To address, the reason for the recipient bounce, and the response code from the recipient host. In addition, you can choose to log a fixed amount of each bounced recipient message. This amount is defined in bytes and the default is zero.
Status Logs	This log file records system statistics found in the CLI status commands, including `status detail` and `dnsstatus`. The period of recording is set using the `setup` subcommand in `logconfig`. Each counter or rate reported in status logs is the value since the last time the counter was reset.
Domain Debug Logs	Domain debug logs record the client and server communication during an SMTP conversation between the Cisco IronPort appliance and a specified recipient host. This log type can be used to debug issues with specific recipient hosts. You must specify the total number of SMTP sessions to record in the log file. As sessions are recorded, this number decreases. You can stop domain debug before all sessions have been recorded by deleting or editing the log subscription.

Table 5-1   Log Types (continued)

Log	Description
Injection Debug Logs	Injection debug logs record the SMTP conversation between the Cisco IronPort appliance and a specified host connecting to the system. Injection debug logs are useful for troubleshooting communication problems between the Cisco IronPort appliance and a host on the Internet.
System Logs	System logs record the following: boot information, DNS status information, and comments users typed using `commit` command. System logs are useful for troubleshooting the basic state of the appliance.
CLI Audit Logs	The CLI audit logs record all CLI activity on the system.
FTP Server Logs	FTP logs record information about the FTP services enabled on the interface. Connection details and user activity are recorded.
HTTP Logs	HTTP logs record information about the HTTP and/or secure HTTP services enabled on the interface. Because the graphical user interface (GUI) is accessed via HTTP, the HTTP logs are ostensibly the GUI equivalent of the CLI Audit logs. Session data (new session, session expired) and pages accessed in the GUI are recorded.
NTP Logs	NTP logs record the conversation between the appliance and any NTP (Network Time Protocol) servers configured. For more information, see "Editing the Network Time Protocol (NTP) Configuration (Time Keeping Method)" in the "System Administration" chapter of the *Cisco IronPort AsyncOS for Email Configuration Guide*.
LDAP Debug Logs	LDAP debug logs are meant for debugging LDAP installations. (See the "LDAP Queries" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.) Useful information about the queries that the Cisco IronPort appliance is sending to the LDAP server are recorded here.

Table 5-1   Log Types (continued)

Log	Description
Anti-Spam Logs	Anti-spam logs record the status of the anti-spam scanning feature of your system, including the status on receiving updates of the latest anti-spam rules. Also, any logs related to the Context Adaptive Scanning Engine are logged here.
Anti-Spam Archive	If you enabled an Anti-Spam scanning feature, messages that are scanned and associated with the "archive message" action are archived here. The format is an mbox-format log file. For more information about anti-spam engines, see the "Anti-Spam" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide.*
Anti-Virus Logs	AntiVirus logs record the status of the anti-virus scanning feature of your system, including the status on receiving updates of the latest anti-virus identity files.
Anti-Virus Archive	If you enabled an anti-virus engine, messages that are scanned and associated with the "archive message" action are archived here. The format is an mbox-format log file. For more information, see the "Anti-Virus" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.
Scanning Logs	The scanning log contains all LOG and COMMON messages for scanning engines (see the Alerts section of the "System Administration" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*). This is typically application faults, alert sent, alert failed, and log error messages. This log does not apply to system-wide alerts.
IronPort Spam Quarantine Logs	IronPort Spam Quarantine logs record actions associated with the IronPort Spam Quarantine processes.
IronPort Spam Quarantine GUI Logs	IronPort Spam Quarantine logs record actions associated with the IronPort Spam Quarantine including configuration via the GUI, end user authentication, and end user actions (releasing email, etc.).
SMTP Conversation Logs	The SMTP conversation log records all parts of incoming and outgoing SMTP conversations.
Safe/Block Lists Logs	Safelist/blocklist logs record data about the safelist/blocklist settings and database.

Table 5-1   Log Types (continued)

Log	Description
Reporting Logs	Reporting logs record actions associated with the processes of the centralized reporting service.
Reporting Query Logs	Reporting query logs record actions associated with the reporting queries that are run on the appliance.
Updater Logs	The updater log records events related to updates for system services, such as McAfee Anti-Virus definition updates.
Tracking Logs	Tracking logs record actions associated with the processes of the tracking service. Tracking logs are a subset of the mail logs.
Authentication Logs	The authentication log records successful user logins and unsuccessful login attempts.

Log Type Characteristics

Table 5-2 summarizes the different characteristics of each log type.

Table 5-2   Log Type Comparison

	Transactional	Stateless	Recorded as text	Recorded as mbox file	Recorded as binary	Periodic Status Information	Message Receiving Information	Delivery Information	Individual Hard Bounces	Individual Soft Bounces	Injection SMTP Conversation	Header Logging	Delivery SMTP Conversation
						Contains							
IronPort Mail Logs	•		•			•	•	•	•	•		•	
qmail Format Delivery Logs		•			•		•	•	•			•	

Table 5-2   *Log Type Comparison (continued)*

	Transactional	Stateless	Recorded as text	Recorded as mbox file	Recorded as binary	Contains							
						Periodic Status Information	Message Receiving Information	Delivery Information	Individual Hard Bounces	Individual Soft Bounces	Injection SMTP Conversation	Header Logging	Delivery SMTP Conversation
Delivery Log		•			•		•	•	•			•	
Bounce Logs	•		•						•	•		•	
Status Logs		•	•			•							
Domain Debug Logs	•		•					•	•	•			•
Injection Debug Logs	•		•				•				•		
System Logs	•		•			•							
CLI Audit Logs	•		•			•							
FTP Server Logs	•		•			•							
HTTP Logs	•		•			•							
NTP Logs	•		•			•							
LDAP Logs	•		•										
Anti-spam logs	•		•			•							
Anti-Spam Archive Logs				•									
Anti-virus Logs	•		•			•							
Anti-Virus Archive				•									

Table 5-2   *Log Type Comparison (continued)*

	Transactional	Stateless	Recorded as text	Recorded as mbox file	Recorded as binary	Contains							
						Periodic Status Information	Message Receiving Information	Delivery Information	Individual Hard Bounces	Individual Soft Bounces	Injection SMTP Conversation	Header Logging	Delivery SMTP Conversation
Scanning Logs	•		•			•							
IronPort Spam Quarantine	•		•			•							
IronPort Spam Quarantine GUI	•		•			•							
Safe/Block Lists Logs	•		•			•							
Reporting Logs	•		•		•								
Reporting Query Logs	•		•		•								
Updater Logs			•										
Tracking Logs	•				•	•	•	•	•	•		•	
Authentication Logs	•		•										

Log Retrieval Methods

Log files can be retrieved based upon one of the following file transfer protocols. You set the protocol while creating or editing the log subscription in the GUI or via the logconfig command during the log subscription process.

Table 5-3   Log Transfer Protocols

FTP Poll	This method involves a remote FTP client accessing the Cisco IronPort appliance to retrieve log files using an admin or operator user's username and password. When configuring a log subscription to use the FTP poll method, you must supply the maximum number of log files to keep on hand. When the maximum number is reached, the system deletes the oldest file.
FTP Push	This method periodically pushes log files to an FTP server on a remote computer. The subscription requires a username, password, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by you. See also *Note About Loading Passwords for Log Subscriptions, page 8-340*.
SCP Push	This method periodically pushes log files to an SCP server on a remote computer. This method requires an SSH SCP server on a remote computer using the SSH1 or SSH2 protocol. The subscription requires a username, SSH key, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by you.
Syslog Push	This method sends log messages to a remote syslog server. This method conforms to RFC 3164. You must submit a hostname for the syslog server and choose to use either UDP or TCP for log transmission. The port used is 514. A facility can be selected for the log; however, a default for the log type is pre-selected in the dropdown menu. Only text-based logs can be transferred using syslog push.

Log Filenames and Directory Structure

IronPort AsyncOS creates a directory for each log subscription based on the log subscription name. The actual name of the log file in the directory is composed of the log filename specified by you, the timestamp when the log file was started, and a single-character status code. The filename of logs are made using the following formula:

    /LogSubscriptionName/LogFilename.@timestamp.statuscode

Status codes may be `.c` (signifying current) or `.s` (signifying saved). You should only transfer log files with the saved status.

Log Rollover and Transfer Schedule

Log subscriptions create and transfer (rollover) log files based on the first user-specified limit reached: maximum file size or maximum time. Log subscriptions based on the FTP poll transfer mechanism will create files and store them in the FTP directory on the Cisco IronPort appliance until they are retrieved or until the system needs more space for log files. See Appendix A, "Accessing the Appliance" for more information.

Logs Enabled by Default

Your IronPort appliance is pre-configured with the following log subscriptions enabled by default (other logs may be configured depending on which license keys you have applied):

Table 5-4   Pre-configured Log Subscriptions

Log #	Log Subscription Name	Log Type	Retrieval Method
1	antispam	Anti-Spam logs	FTP Poll
2	antivirus	Anti-Virus Logs	FTP Poll
3	asarchive	Anti-Spam Archive	FTP Poll
4	authentication	Authentication Logs	FTP Poll
5	avarchive	Anti-Virus Archive	FTP Poll
6	bounces	Bounce Logs	FTP Poll

Table 5-4   Pre-configured Log Subscriptions (continued)

Log #	Log Subscription Name	Log Type	Retrieval Method
7	`cli_logs`	CLI Audit Logs	FTP Poll
8	`encryption`	Encryption	FTP Poll
9	`error_logs`	IronPort Text Mail Logs	FTP Poll
10	`euq_logs`	IronPort Spam Quarantine Logs	FTP Poll
11	`euqgui_logs`	IronPort Spam Quarantine GUI Logs	FTP Poll
12	`ftpd_logs`	FTP Server Logs	FTP Poll
13	`gui_logs`	HTTP Logs	FTP Poll
14	`mail_logs`	IronPort Text Mail Logs	FTP Poll
15	`reportd_logs`	Reporting Logs	FTP Poll
16	`reportingqueryd_logs`	Reporting Query Logs	FTP Poll
17	`scanning`	Scanning Logs	FTP Poll
18	`slbld_logs`	Safe/Block Lists Logs	FTP Poll
19	`sntpd_logs`	NTP logs	FTP Poll
20	`status`	Status Logs	FTP Poll
21	`system_logs`	System Logs	FTP Poll
22	`trackerd_logs`	Tracking Logs	FTP Poll
23	`updater_logs`	Updater Logs	FTP Poll

All pre-configured log subscriptions have a Log Level of 3, except for `error_logs` which is set at 1 so that it will contain only errors. See Log Levels, page 5-207 for more information. For information about creating new log subscriptions, or modifying existing ones, see Log Subscriptions, page 5-206.

Log Types

This section covers the following topics:

Timestamps in Log Files

The following log files include the begin and end date of the log itself, the version of AsyncOS, and the GMT offset (provided in seconds, and only at the beginning of the log):

- Anti-Virus log

- LDAP log
- System log
- Mail log

Using IronPort Text Mail Logs

These logs do not require any special configuration. They contain details of email receiving, email delivery and bounces. Status information is also written to the mail log every minute. These logs are a useful source of information to understand delivery of specific messages and to analyze system performance.

Information displayed in text mail logs is shown in Table 5-5.

Table 5-5   *Text Mail Log Statistics*

Statistic	Description
ICID	Injection Connection ID. This is a numerical identifier for an individual SMTP connection to the system, over which 1 to thousands of individual messages may be sent.
DCID	Delivery Connection ID. This is a numerical identifier for an individual SMTP connection to another server, for delivery of 1 to thousands of messages, each with some or all of their RIDs being delivered in a single message transmission.
RCID	RPC Connection ID. This is a numerical identifier for an individual RPC connection to the IronPort Spam quarantine. It is used to track messages as they are sent to and from the IronPort Spam Quarantine.
MID	Message ID: Use this to track messages as they flow through the logs.
RID	Recipient ID: Each message recipient is assigned an ID.
New	New connection initiated.
Start	New message started.

Interpreting an IronPort Text Mail Log

Use the following sample as a guide to interpret log files.

Note Individual lines in log files are NOT numbered. They are numbered here only for sample purposes.

Table 5-6   Text Mail Log Detail

1	Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes
2	Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
3	Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>
4	Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>
5	Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>
6	Mon Apr 17 19:59:59 2003 Info: ICID 5 close
7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

Use Table 5-7 as a guide to reading the preceding log file.

Table 5-7   Detail of Text Mail Log Example

Line Number	Description
1.	A new connection is initiated into the system and assigned an Injection ID (ICID) of "5." The connection was received on the Management IP interface and was initiated from the remote host at 10.1.1.209.
2.	The message was assigned a Message ID (MID) of "6" after the MAIL FROM command is issued from the client.
3.	The sender address is identified and accepted.
4.	The recipient is identified and assigned a Recipient ID (RID) of "0."

Table 5-7   Detail of Text Mail Log Example (continued)

Line Number	Description
5.	MID 5 is accepted, written to disk, and acknowledged.
6.	Receiving is successful and the receiving connection closes.
7.	Next the message delivery process starts. It is assigned a Delivery Connection ID (DCID) of "8" from 192.168.42.42 and to 10.5.3.25.
8.	The message delivery starts to RID "0."
9.	Delivery is successful for MID 6 to RID "0."
10.	The delivery connection closes.

Examples of Text Mail Log Entries

Following are some sample log entries based on various situations.

Message Injection and Delivery

A message is injected into the Cisco IronPort appliance for a single recipient. The message is successfully delivered.

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface
mail.example.com (1.2.3.4) address 2.3.4.5 reverse dns host unknown
verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None

Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From:
<someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To:
<user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
```

```
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from
<someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface
1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID
200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID
200257070 to RID [0] [('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

Successful Message Delivery

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11
address 63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

Unsuccessful Message Delivery (Hard Bounce)

A message with two recipients is injected into the Cisco IronPort appliance. Upon delivery, the destination host returns a 5*XX* error, which indicates that the message cannot be delivered to either recipient. The Cisco IronPort appliance notifies the sender and removes the recipients from the queue.

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11
address 64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0,
1]

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0
- Unknown address error ('550', ['<george@yourdomain.com>... Relaying
denied']) []

Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0
- Unknown address error ('550', ['<jane@yourdomain.com>... Relaying
denied']) []

Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

Soft Bounce Followed by Successful Delivery

A message is injected into the Cisco IronPort appliance. On the first delivery attempt, the message soft bounces and is queued for future delivery. On the second attempt, the message is successfully delivered.

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11
address 63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0,
1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0
- Unknown address error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon
Mar 31 20:01:23 2003

Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet
address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID
[0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

Message Scanning Results for the scanconfig Command

You can use the `scanconfig` command to determine the system behavior when a message can not be deconstructed into its component parts (when removing attachments). The Options are `Deliver`, `Bounce`, or `Drop`.

The following example shows the IronPort Text Mail log with `scanconfig` set to `Deliver`.

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From:
<test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To:
<joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID
'<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test
#22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from
<test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem:
Continuation line seen before first header

Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive
'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by
antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

The following example shows the IronPort Tex Mail log with `scanconfig` set to `drop`.

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To:
<joe@example.com>

Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID
'<392912.@virus.org>'
```

```
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test
#22'

Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from
<test@virus.org>

Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem:
Continuation line seen before first header

Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by
filter 'drop_zip_c'

Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done

Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

Log Entries for Generated or Re-Written Messages

Some functions, such as rewrite/redirect actions (`alt-rcpt-to` filters, anti-spam rcpt rewrite, `bcc()` actions, anti-virus redirections, etc.), create new messages. When looking through the logs, you might need to check the results and add in further MIDs and possibly DCIDs. Entries such as these are possible:

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by
bcc filter 'nonetest'
```

or:

```
Tue Jan  6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by
alt-rcpt-to-filter filter 'testfilt'
```

An interesting point to note about 'rewritten' entries is that they can appear after lines in the log indicating use of the new MID.

Messages Sent to the IronPort Spam Quarantine

When you send a message to the quarantine, the mail logs track the movement to and from the quarantine using the RCID (RPC connection ID) to identify the RPC connection. In the following mail log, a message is tagged as spam, and sent to the IronPort Spam Quarantine:

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From:
<HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.
chase.com>'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream
home - Now make it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from
<HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for
per-recipient policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam
suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine

Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative

Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery

Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID
2317877 to local IronPort Spam Quarantine

Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
```

```
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877

Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

Using IronPort Delivery Logs

Delivery logs record critical information about the email delivery operations of
AsyncOS. The log messages are "stateless," meaning that all associated
information is recorded in each log message and users need not reference previous
log messages for information about the current delivery attempt.

The delivery log records all information pertaining to email delivery operations
for each recipient. All information is laid out in a logical manner and is
human-readable after conversion using a utility provided by IronPort. The
conversion tools are located at:

http://support.ironport.com

Delivery logs are recorded and transferred in a binary format for resource
efficiency. Information recorded in delivery logs is shown in the following table:

Table 5-8   Delivery Log Statistics

Statistic	Description
Delivery status	Success (message was successfully delivered) or bounce (message was hard bounced)
Del_time	Delivery time
Inj_time	Injection time. del_time - inj_time = time the recipient message stayed in the queue
Bytes	Message size
Mid	Message ID
Ip	Recipient host IP. The IP address of the host that received or bounced the recipient message
From	Envelope From, also known as Envelope Sender or MAIL FROM
Source_ip	Source host IP. The IP address of the host of the incoming message
Code	SMTP response code from recipient host

Table 5-8   Delivery Log Statistics (continued)

Statistic	Description
Reply	SMTP response message from recipient host
Rcpt Rid	Recipient ID. Recipient ID starts with <0>, messages with multiple recipients will have multiple recipient IDs
To	Envelope To
Attempts	Number of delivery attempts

If the delivery status was bounce, this additional information appears in the delivery log:

Table 5-9   Delivery Log Bounce Information

Statistic	Description
Reason	RFC 1893 Enhanced Mail Status Code interpretation of the SMTP response during the delivery
Code	SMTP response code from recipient host
Error	SMTP response message from recipient host

If you have set up logheaders (see), the header information appears after the delivery information:

Table 5-10   Delivery Log Header Information

Statistic	Description
Customer_data	XML tag marking the beginning of logged headers
Header Name	Name of the header
Value	Contents of the logged header

Examples of Delivery Log Entries

The examples in this section show a variety of Delivery Log entries.

Successful Message Delivery

```
<success del_time="Fri Jan 09 15:34:20.234 2004" inj_time="Fri Jan 09
15:33:38.623 2004" bytes="202" mid="45949" ip="10.1.1.1"
from="campaign1@yourdomain.com" source_ip="192.168.102.1" code="250"
reply="sent">

<rcpt rid="0" to="alsdfj.ajsdfl@alsdfj.d2.qa25.qa" attempts="1" />

</success>
```

Delivery Status Bounce

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05
08:28:32.929 2003" bytes="4074" mid="94157762" ip="0.0.0.0"
from="campaign1@yourdomain.com" source_ip="192.168.102.1 "reason="5.1.0 -
Unknown address error" code="550" error="["Requested action not taken:
mailbox unavailable"]">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

Delivery Log Entry with Logheaders

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28
15:55:17.696 2003" bytes="139" mid="202" ip="10.1.1.13"
from="campaign1@yourdomain.com" source_ip="192.168.102.1" code="250"
reply="sent">

<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

Using IronPort Bounce Logs

The bounce log records all information pertaining to each bounced recipient. Information recorded in bounce logs is shown in Table 5-11.

Table 5-11   *Bounce Log Statistics*

Statistic	Description
Timestamp	The time of the bounce event
Log level	The level of detail in this bounce log
Bounce type	Bounced or delayed (for example, hard or soft-bounce)
MID/RID	Message ID and recipient ID
From	Envelope From
To	Envelope To
Reason	RFC 1893 Enhanced Mail Status Code interpretation of the SMTP response during the delivery
Response	SMTP response code and message from recipient host

In addition, if you have specified message size to log or setup logheaders (see Logging Message Headers, page 5-212), the message and header information will appear after the bounce information:

Table 5-12   *Bounce Log Header Information*

Header	The header name and content in the header
Message	Content of the message logged

Examples of Bounce Log Entries

Soft-Bounced Recipient (Bounce Type = Delayed)

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>
```

```
Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

Hard-Bounced Recipient (Bounce Type = Bounced)

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0
From:<campaign1@yourdomain.com> To:<user2@sampledomain.com>
```

```
Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no
such active account.'])"
```

Bounce Log with Message Body and Logheaders

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>

Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers:
['xname: userID2333']' Message: Message-Id:
```

```
<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

Note   The text string \015\012 represents a line break (for example, CRLF).

Using IronPort Status Logs

Status logs record system statistics found in the CLI status commands, including `status`, `status detail`, and `dnsstatus`. The period of recording is set using the `setup` subcommand in `logconfig`. Each counter or rate reported in status logs is the value since the last time the counter was reset.

Reading Status Logs

Table 5-13 table shows the status log labels and the matching system statistics.

Table 5-13   ***Status Log Statistics***

Statistic	Description
CPULd	CPU Utilization
DskIO	Disk I/O Utilization
RAMUtil	RAM Utilization
QKUsd	Queue Kilobytes Used
QKFre	Queue Kilobytes Free
CrtMID	Message ID (MID)
CrtICID	Injection Connection ID (ICID)
CRTDCID	Delivery Connection ID (DCID)
InjMsg	Injected Messages
InjRcp	Injected Recipients
GenBncRcp	Generated Bounce Recipients
RejRcp	Rejected Recipients
DrpMsg	Dropped Messages
SftBncEvnt	Soft Bounced Events
CmpRcp	Completed Recipients

Table 5-13   Status Log Statistics (continued)

Statistic	Description
HrdBncRcp	Hard Bounced Recipients
DnsHrdBnc	DNS Hard Bounces
5XXHrdBnc	5XX Hard Bounces
FltrHrdBnc	Filter Hard Bounces
ExpHrdBnc	Expired Hard Bounces
OtrHrdBnc	Other Hard Bounces
DlvRcp	Delivered Recipients
DelRcp	Deleted Recipients
GlbUnsbHt	Global Unsubscribe Hits
ActvRcp	Active Recipients
UnatmptRcp	Unattempted Recipients
AtmptRcp	Attempted Recipients
CrtCncIn	Current Inbound Connections
CrtCncOut	Current Outbound Connections
DnsReq	DNS Requests
NetReq	Network Requests
CchHit	Cache Hits
CchMis	Cache Misses
CchEct	Cache Exceptions
CchExp	Cache Expired
CPUTTm	Total CPU time used by the application
CPUETm	Elapsed time since the application started
MaxIO	Maximum disk I/O operations per second for the mail process
RamUsd	Allocated memory in bytes
SwIn	Memory swapped in.
SwOut	Memory swapped out.

Table 5-13   Status Log Statistics (continued)

Statistic	Description
SwPgIn	Memory paged in.
SwPgOut	Memory paged out.
MMLen	Total number of messages in the system
DstInMem	Number of destination objects in memory
ResCon	Resource conservation tarpit value. Acceptance of incoming mail is delayed by this number of seconds due to heavy system load
WorkQ	This is the number of messages currently in the work queue
QuarMsgs	Number of individual messages in system quarantine (messages present in multiple quarantines are counted only once)
QuarQKUsd	KBytes used by system quarantine messages
LogUsd	Percent of log partition used
AVLd	Percent CPU used by anti-virus scanning
CmrkLd	Percent CPU used by Cloudmark anti-spam scanning
SophLd	Percent CPU used by Sophos anti-spam scanning
McafLd	Percent CPU used by McAfee anti-virus scanning
CASELd	Percent CPU used by CASE scanning
TotalLd	Total CPU consumption
LogAvail	Amount of disk space available for log files
EuQ	Estimated number of messages in the IronPort Spam quarantine
EuqRls	Estimated number of messages in the IronPort Spam quarantine release queue

Status Log Example

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0
QKFre 8388608 CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp
14230 GenBncRcp 12 RejRcp 6318 DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813
HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc 0 ExpHrdBnc 1 OtrHrdBnc
0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0
CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis
504791 CchEct 15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350
RAMUsd 21528056 MMLen 0 DstInMem 4 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd
0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail 17G EuQ 0 EuqRls 0
```

Using IronPort Domain Debug Logs

Domain debug logs record the client and server communication during an SMTP conversation between the Cisco IronPort appliance and a specified recipient host. This log type is primarily used to debug issues with specific recipient hosts.

Table 5-14　　*Domain Debug Log Statistics*

Statistic	Description
Timestamp	The time of the bounce event
Log level	The level of detail in this bounce log
From	Envelope From
To	Envelope To
Reason	RFC 1893 Enhanced Mail Status Code interpretation of the SMTP response during the delivery
Response	SMTP response code and message from recipient host

Domain Debug Log Example

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL
FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT
TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END
WITH "." ON A LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

Using IronPort Injection Debug Logs

Injection debug logs record the SMTP conversation between the Cisco IronPort appliance and a specified host connecting to the system. Injection debug logs are useful for troubleshooting communication problems between the Cisco IronPort appliance and a client initiating a connection from the Internet. The log records all bytes transmitted between the two systems and classifies them as "Sent to" the connecting host or "Received from" the connecting host.

You must designate the host conversations to record by specifying an IP address, an IP range, hostname, or partial hostname. Any connecting IP address within an IP range will be recorded. Any host within a partial domain will be recorded. The system performs reverse DNS lookups on connecting IP addresses to convert to hostnames. IP addresses without a corresponding PTR record in DNS will not match hostnames.

You must also specify the number of sessions to record.

Each line within an Injection Debug log contains the following information in
Table 5-15.

Table 5-15   *Injection Debug Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
ICID	The Injection Connection ID is a unique identifier that can be tied to the same connection in other log subscriptions
Sent/Received	Lines marked with "Sent to" are the actual bytes sent to the connecting host. Lines marked with "Received from" are the actual bytes received from the connecting host
IP Address	IP address of the connecting host

Injection Debug Log Example

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220
postman.example.com ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go
ahead\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject:
Test Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the
content of the message'

Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'
```

Using IronPort System Logs

Table 5-16   *System Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The logged event

System Log Example

In this example, the System log shows some commit entries, including the name of the user issuing the commit and the comment entered.

```
Wed Sep  8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep  8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep  8 18:02:45 2004 Info: System is coming up

Wed Sep  8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep  8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep  8 18:13:30 2004 Info: PID 608: User admin commit changes:
SSW:Password

Wed Sep  8 18:17:23 2004 Info: PID 608: User admin commit changes:
Completed Web::SSW

Thu Sep  9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep  9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added
a second CLI log for examples

Thu Sep  9 08:51:53 2004 Info: PID 1237: User admin commit changes:
Removed example CLI log.
```

Using IronPort CLI Audit Logs

Table 5-17   *CLI Audit Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
PID	Process ID for the particular CLI session in which the command was entered
Message	The message consists of the CLI command entered, the CLI output (including menus, lists, etc.), and the prompt that is displayed

CLI Audit Log Example

In this example, the CLI Audit log shows that, for PID 16434, the following CLI commands were entered: who, textconfig.

```
Thu Sep  9 14:35:55 2004 Info: PID 16434: User admin entered 'who';
prompt was '\nmail3.example.com> '

Thu Sep  9 14:37:12 2004 Info: PID 16434: User admin entered
'textconfig'; prompt was '\nUsername  Login Time  Idle Time  Remote Host
What\n========  ==========  =========  ===========  ====\nadmin    Wed
11AM   3m 45s    10.1.3.14    tail\nadmin    02:32PM    0s
10.1.3.14    cli\nmail3.example.com> '

Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt
was '\nThere are no text resources currently defined.\n\n\nChoose the
operation you want to perform:\n- NEW - Create a new text resource.\n-
IMPORT - Import a text resource from a file.\n[]> '
```

Using IronPort FTP Server Logs

Table 5-18 **FTP Server Log Statistics**

Statistic	Description
Timestamp	Time that the bytes were transmitted
ID	Connection ID. A separate ID for each FTP connection
Message	The message section of the log entry can be logfile status information, or FTP connection information (login, upload, download, logout, etc.)

FTP Server Log Example

In this example, the FTP Server log records a connection (ID:1). The IP address of the incoming connection is shown, as well as the activity (uploading and downloading files) and the logout.

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile

Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN:
00065BF3BA6D-9WFWC21

Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep  8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on
172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes

Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

Using IronPort HTTP Logs

Table 5-19   ***HTTP Log Statistics***

Statistic	Description
Timestamp	Time that the bytes were transmitted
ID	Session ID
req	IP address of machine connecting
user	Username of user connecting
Message	Information regarding the actions performed. May include GET or POST commands or system status, etc.

HTTP Log Example

In this example, the HTTP log shows the admin user's interaction with the GUI (running the System Setup Wizard, etc.).

```
Wed Sep  8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting
to https port 443

Wed Sep  8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep  8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep  8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep  8 11:17:24 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg POST /system_administration/system_setup_wizard
HTTP/1.1 303

Wed Sep  8 11:17:25 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /system_administration/ssw_done HTTP/1.1 200

Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin
&height=190 HTTP/1.1 200
```

```
Wed Sep  8 11:18:46 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipie
ntsin&height=190 HTTP/1.1 200

Wed Sep  8 11:18:49 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /monitor/quarantines HTTP/1.1 200
```

Using IronPort NTP Logs

Table 5-20   *NTP Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The message consists of either a Simple Network Time Protocol (SNTP) query to the server, or an adjust: message

NTP Log Example

In this example, the NTP log shows the appliance polling the NTP host twice.

```
Thu Sep  9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset
-652

Thu Sep  9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us
next_poll: 4096

Thu Sep  9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset
-1152

Thu Sep  9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us
next_poll: 4096
```

Using IronPort Anti-Spam Logs

Table 5-21   *Anti-Spam Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The message consists of the check for the anti-spam updates, as well as the results (whether an update of the engine or the anti-spam rules was needed, etc.)

Anti-Spam Log Example

In this example, the anti-spam log shows the anti-spam engine checking for updates to spam definitions and CASE updates::

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) :
case-daemon: server successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) :
startup: Region profile: Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy:
Fuzzy plugin v7 successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) :
uribllocal: running URI blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config:
Finished loading configuration
```

Using IronPort Anti-Virus Logs

Table 5-22   *AntiVirus Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The message consists of the check for the anti-virus update, as well as the results (whether an update of the engine or the virus definitions was needed, etc.)

Anti-Virus Log Example

In this example, the Anti-Virus log shows the Sophos anti-virus engine checking for updates to virus definitions (IDE) and the engine itself.

```
Thu Sep  9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep  9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine
update needed

Thu Sep  9 14:18:04 2004 Info: Current IDE serial=2004090902. No update
needed.
```

You can temporarily set this to DEBUG level to help diagnose why the anti-virus engine returns a particular verdict for a given message. The DEBUG logging information is verbose; use with caution.

Using IronPort Spam Quarantine Logs

Table 5-23   *IronPort Spam Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The message consists of actions taken (messages quarantined, released from quarantine, etc.).

IronPort Spam Quarantine Log Example

In this example, the log shows a message (MID 8298624) being released from the quarantine to admin@example.com.

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for
all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624
(skipping work queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to
admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625
(skipping work queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to
admin@example.com
```

Using IronPort Spam Quarantine GUI Logs

Table 5-24   IronPort Spam GUI Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The message consists of actions taken, including user authentication, etc.

IronPort Spam Quarantine GUI Log Example

In this example, the log shows a successful authentication, login and logout:

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port
82

Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1,
port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

Using IronPort LDAP Debug Logs

Table 5-25   *LDAP Debug Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	LDAP Debug message

LDAP Debug Log Example

✎

Note   Individual lines in log files are NOT numbered. They are numbered here only for sample purposes

```
1    Thu Sep  9 12:24:56 2004 Begin Logfile

2    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

3    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

4    Thu Sep  9 12:25:02 2004 LDAP: Masquerade query sun.masquerade
     address employee@routing.qa to employee@mail.qa

5    Thu Sep  9 12:28:08 2004 LDAP: Clearing LDAP cache

6    Thu Sep  9 13:00:09 2004 LDAP: Query
     '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun
     (sun.qa:389)

7    Thu Sep  9 13:00:09 2004 LDAP: After substitute, query is
     '(&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d000
     02b.loc@ldap.route.local.add00002.qa))'

8    Thu Sep  9 13:00:09 2004 LDAP: connecting to server

9    Thu Sep  9 13:00:09 2004 LDAP: connected
```

```
10    Thu Sep  9 13:00:09 2004 LDAP: Query
      (&(ObjectClass=inetLocalMailRecipient)(mailLocalAddress=rroute.d0000
      2b.loc@ldap.route.local.add00002.qa)) returned 1 results

11    Thu Sep  9 13:00:09 2004 LDAP: returning: [<LDAP:>]
```

Use as a guide to reading the preceding log file.

Table 5-26   Detail of LDAP Debug Log Example

Line Number	Description
1.	The log file is initialized.
2. 3. 4.	The listener is configured to use LDAP for masquerading, specifically with the LDAP query named "sun.masquerade." The address employee@routing.qa is looked up in the LDAP server, a match is found, and the resulting masquerade address is employee@mail.qa, which will be written to the message headers and/or the envelope from, depending on the masquerade configuration.
5.	The user has manually run `ldapflush`.
6.	A query is about to be sent to sun.qa, port 389. The query template is: (&(ObjectClass={g})(mailLocalAddress={a})). The {g} will be replaced by the groupname specified in the calling filter, either a rcpt-to-group or mail-from-group rule. The {a} will be replaced by the address in question.
7. 8.	Now the substitution (described previously) takes place, and this is what the query looks like before it is sent to the LDAP server.
9.	The connection to the server is not yet established, so make a connection.

Table 5-26   Detail of LDAP Debug Log Example (continued)

Line Number	Description
10.	The data that is sent to the server.
11.	The result is an empty positive, meaning one record was returned, but since the query didn't ask for any fields, there is no data to report. These are used for both group and accept queries when the query checks to see if there is a match in the database.

Using Safelist/Blocklist Logs

Table 5-27 shows the statistics recorded in safelist/blocklist logs.

Table 5-27   Safelist/Blocklist Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted.
Message	The message consists of actions taken, including user authentication, and so forth.

Safelist/Blocklist Log Example

In this example, the safelist/blocklist log shows the appliance creating database snapshots every two hours. It also shows when senders were added to the database.

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007
Info: Version: 6.0.0-425 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007
Info: Time offset from UTC: 10800 seconds Fri Sep 28 14:22:33 2007 Info:
System is coming up.

Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been
created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been
created.

Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been
created.
```

```
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been
created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been
created.

.........................

Mon Oct  1 14:16:09 2007 Info: SLBL: The database snapshot has been
created.

Mon Oct  1 14:37:39 2007 Info: SLBL: The database snapshot has been
created.

Mon Oct  1 15:31:37 2007 Warning: SLBL: Adding senders to the database
failed.

Mon Oct  1 15:32:31 2007 Warning: SLBL: Adding senders to the database
failed.

Mon Oct  1 16:37:40 2007 Info: SLBL: The database snapshot has been
created.
```

Using Reporting Logs

Table 5-28 shows the statistics recorded in reporting logs.

Table 5-28   Reporting Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted.
Message	The message consists of actions taken, including user authentication, and so forth.

Reporting Log Example

In this example, the Reporting log shows the appliance set at the information log level.

```
Wed Oct  3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct  3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct  3 13:40:02 2007 Info: Update 2 registered appliance at
2007-10-03-13-40

Wed Oct  3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not
found: 1692

Wed Oct  3 13:40:53 2007 Info: Period hour using 36800 (KB)

Wed Oct  3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct  3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct  3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct  3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533
seconds

Wed Oct  3 13:41:02 2007 Info: Update 2 registered appliance at
2007-10-03-13-41

Wed Oct  3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not
found: 1692

Wed Oct  3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct  3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct  3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct  3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct  3 13:42:03 2007 Info: Update 2 registered appliance at
2007-10-03-13-42
```

Using Reporting Query Logs

Table 5-29 shows the statistics recorded in reporting query logs.

Table 5-29   *Reporting Query Log Statistics*

Statistic	Description
Timestamp	Time that the bytes were transmitted.
Message	The message consists of actions taken, including user authentication, and so forth.

Reporting Query Log Example

In this example, the reporting query log shows the appliance running a daily outgoing email traffic query for the period from August 29 to October 10, 2007.

```
Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct  2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610229
for ['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTEN

T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI

PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29
to 2007-10-01 with key constraints

 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM']
returning results from 0 to 2 sort_ascendin

g=False.

Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610229.
```

```
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610230
for ['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM

ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range
2007-08-29 to 2007-10-01 with key constra

ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES']
returning results from 0 to 2 sort

_ascending=False.

Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

Using Updater Logs

Table 5-30   Updater Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted.
Message	The message consists of system service update information, as well as AsyncOS checking for updates and the scheduled date and time of the next update.

Updater Log Example

In this example, the logs show the appliance being updated with new McAfee Anti-Virus definitions.

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update
11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for
mcafee
```

```
Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server
manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:12:52 2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:17:52 2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep
19 11:22:52 2008
```

Understanding Tracking Logs

Tracking logs record information about the email operations of AsyncOS. The log messages are a subset of the messages recorded in the mail logs.

The tracking logs are used by the message tracking component to build the message tracking database. Because the log files are consumed in the process of building the database, the tracking logs are transient. The information in tracking logs is not designed to be read or analyzed by humans.

Tracking logs are recorded and transferred in a binary format for resource efficiency. The information is laid out in a logical manner and is human-readable after conversion using a utility provided by IronPort. The conversion tools are located at the following URL:

```
http://tinyurl.com/3c5l8r
```

Using Authentication Logs

The authentication log records successful user logins and unsuccessful login attempts.

Table 5-31   Authentication Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted.
Message	The message consists of the username of a user who attempted to log in to the appliance and whether the user was authenticated successfully.

Authentication Log Example

In this example, the log shows the log in attempts by users "admin," "joe," and "dan."

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX

Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds
```

```
Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

Log Subscriptions

This section contains the following topics:

Configuring Log Subscriptions

Use the Log Subscriptions page on the System Administration menu (or the `logconfig` command in the CLI) to configure a log subscription. Log subscriptions create log files that store information about AsyncOS activity,

including errors. A log subscription is either delivered to (pushed) or retrieved from (polled) another computer. Generally, log subscriptions have the following attributes:

Table 5-32   Log File Attributes

Attribute	Description
Log type	Defines the type of information recorded and the format of the log subscription. See Table 5-1, "Log Types," on page 156 for more information.
Name	Nickname for the log subscription to be used for your future reference.
Log level	Sets the level of detail for each log subscription.
Retrieval method	Defines how the log subscription will be transferred from of the Cisco IronPort appliance.
Log filename	Used for the physical name of the file when written to disk. If multiple Cisco IronPort appliances are being used, the log filename should be unique to identify the system that generated the log file.
Maximum File Size	The maximum size the file can reach before rolling over.

Log Levels

Log levels determine the amount of information delivered in a log. Logs can have one of five levels of detail. A more detailed setting creates larger log files and puts more drain on system performance. More detailed settings include all the messages contained in less detailed settings, plus additional messages. As the level of detail increases, system performance decreases.

Note Log levels may be selected for all mail log types.

Table 5-33   Log Levels

Log Level	Description
Critical	The least detailed setting. Only errors are logged. Using this setting will not allow you to monitor performance and other important activities; however, the log files will not reach their maximum size as quickly. This log level is equivalent to the syslog level "Alert."
Warning	All errors and warnings created by the system. Using this setting will not allow you to monitor performance and other important activities. This log level is equivalent to the syslog level "Warning."
Information	The information setting captures the second-by-second operations of the system. For example, connections opened or delivery attempts. The Information level is the recommended setting for logs. This log level is equivalent to the syslog level "Info."
Debug	Use the Debug log level when you are trying to discover the cause of an error. Use this setting temporarily, and then return to the default level. This log level is equivalent to the syslog level "Debug."
Trace	The Trace log level is recommended only for developers. Using this level causes a serious degradation of system performance and is not recommended. This log level is equivalent to the syslog level "Debug."

Creating a Log Subscription in the GUI

To create a log subscription,

Step 1 Click **Add Log Subscription** on the Log Subscription page. The New Log Subscription page is displayed:

Figure 5-1   Creating a New Log Subscription

New Log Subscription

Log Subscription	
Log Type:	Select a log type... ▼
Log Name:	[ ]
	(will be used to name the log directory)
File Name:	[ ]
Maximum File Size:	[10M]
	(Add a trailing K or M to indicate size units)
Log Level:	○ Critical (The least detailed setting. Only errors are logged.)
	○ Warning (All errors and warnings created by the system.)
	⦿ Information (Captures the second-by-second operations of the system. Recommended.)
	○ Debug (More specific data are logged to help debug specific problems.)
	○ Trace (The most detailed setting, all information that can be is logged. Recommended for developers only.)
Retrieval Method:	⦿ FTP on test28.eng
	Maximum Number of Files: [10]
	○ FTP on Remote Server
	Maximum Time Interval Between Transferring: [3600] seconds
	FTP Host: [ ]
	Directory: [ ]
	Username: [ ]
	Password: [ ]
	○ SCP on Remote Server
	Maximum Time Interval Between Transfering: [3600] seconds
	Protocol: ○ SSH1 ⦿ SSH2
	SCP Host: [ ]
	Directory: [ ]
	Username: [ ]
	☐ Enable Host Key Checking
	⦿ Automatically Scan
	○ Enter Manually
	[ ]

Cancel   Submit

Step 2   Select a log type and enter the log name (for the log directory) as well as the name for the log file itself.

Step 3   Specify the maximum file size as well as the log level.

Step 4   Configure the log retrieval method.

Step 5   Submit and commit your changes.

Editing Log Subscriptions

To edit a log subscription:

Step 1   Click the name of the log in the Log Name column on the Log Subscriptions page.
The Edit Log Subscription page is displayed.

Step 2   Make changes to the log subscription.

Step 3   Submit and commit your changes.

Configuring Global Settings for Logging

The system periodically records system measurements within the IronPort Text
Mail Logs and the IronPort Status Logs. Use the **Edit Settings** button in the
Global Settings section of the System Administration > Log Subscriptions page
(or the logconfig -> setup command in the CLI) to configure:

- System metrics frequency. This is the amount of time, in seconds, that the
  system waits between recording measurements.

- Whether to record the Message-ID headers.

- Whether to record the remote response status code.

- Whether to record the subject header of the original message.

- A list of headers that should be logged for each message.

All IronPort logs optionally include the following three pieces of data:

1. Message-ID

When this option is configured, every message will have its Message ID header logged, if it is available. Note that this Message-ID may have come from the received message or may have been generated by AsyncOS itself. For example:

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

2. Remote Response

When this option is configured, every message will have its remote response status code logged, if it is available. For example:

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as
9C8B425DA7'
```

The remote response string is the human-readable text received after the response to the DATA command during the delivery SMTP conversation. In this example, the remote response after the connection host issued the data command is "queued as 9C8B425DA7."

```
[...]

250 ok hostname

250 Ok: queued as 9C8B425DA7
```

Whitespace, punctuation, (and in the case of the 250 response, the OK characters) are stripped from the beginning of the string. Only whitespace is stripped from the end of the string. For example, IronPort appliances, by default, respond to the DATA command with this string: 250 Ok: Message MID accepted. So, the string "Message MID accepted" would be logged if the remote host were another IronPort appliance.

3. Original Subject Header

When this option is enabled, the original subject header of each message is included in the log.

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>

Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'

Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

Logging Message Headers

In some cases, it is necessary to record the presence and contents of a message's headers as they pass through the system. You specify the headers to record in the Log Subscriptions Global Settings page (or via the `logconfig -> logheaders` subcommand in the CLI). The Cisco IronPort appliance records the specified message headers in the IronPort Text Mail Logs, the IronPort Delivery Logs, and the IronPort Bounce Logs. If the header is present, the system records the name of the header and the value. If a header is not present, nothing is recorded in the logs.

Note   The system evaluates all headers that are present on a message, at any time during the processing of the message for recording, regardless of the headers specified for logging.

Note   The RFC for the SMTP protocol is located at `http://www.faqs.org/rfcs/rfc2821.html` and defines user-defined headers.

Note   If you have configured headers to log via the `logheaders` command, the header information appears after the delivery information:

Table 5-34   Log Headers

Header name	Name of the header
Value	Contents of the logged header

For example, specifying "date, x-subject" as headers to be logged will cause the following line to appear in the mail log:

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this
header')]
```

Configuring Global Settings for Logging via the GUI

To configure global settings for logging,

Step 1   Click the **Edit Settings** button in the Global Settings section of the Log Subscriptions page. The Log Subscriptions Global Settings page is displayed:

Figure 5-2   Configuring Log Subscriptions Global Settings

Log Subscriptions Global Settings

Edit Global Settings	
System measurements frequency:	`45` seconds
Logging Options:	☑ Message-ID headers in Mail Logs:
	☑ Original subject header of each message:
	☑ Remote response text in Mail Logs:
Headers (Optional):	List any headers you want to record in the log files: date x-subject

Cancel   Submit

Step 2   Specify the system measurement frequency, whether to include Message-ID headers in mail logs, whether to include the remote response, and whether to include the original subject header of each message.

Step 3   Enter any other headers you wish to include in the logs.

Step 4   Submit and commit your changes.

Rolling Over Log Subscriptions

IronPort AsyncOS rolls over log files based on settings you configure on the Log Subscriptions Global Settings page (or with the `logconfig` command in the CLI). Log files can also be rolled on demand by clicking the **Rollover Now** button on the Log Subscriptions page or by using the `rollovernow` command. When IronPort AsyncOS rolls over a log file, it:

- Creates a new log file with the timestamp of the rollover and designates the file as current with the letter "**c**" extension

- Renames the current log file to have a letter "**s**" extension signifying saved

- Transfers the newly saved log file to a remote host (if push-based)

- Transfers any previously unsuccessful log files from the same subscription (if push-based)

- Deletes the oldest file in the log subscription if the total number of files to keep on hand has been exceeded (if poll-based)

Rolling Over Log Subscriptions via the GUI

To roll over log subscriptions,

Step 1 On the Log Subscriptions page, mark the checkbox to the right of the logs you wish to roll over.

Step 2 Optionally, you can select all logs for rollover by marking the All checkbox.

Step 3 Once one or more logs have been selected for rollover, the **Rollover Now** button is enabled. Click the **Rollover Now** button to roll over the selected logs.

Rolling Over Log Subscriptions via the CLI

The `rollovernow` command allows you to roll over all log files at once or select a specific log file from a list.

Viewing Recent Log Entries in the GUI

You can view a log file via the GUI by clicking on the log subscription in the Log Files column of the table on the Log Subscriptions page. When you click on the link to the log subscription, you are asked to enter your password and then a listing of log files for that subscription is displayed. You can then click on one of the log files to view it in your browser or to save it to disk. You must have the FTP service enabled on the Management interface in order to view logs via the GUI.

Figure 5-3   *Configuring Log Subscriptions Global Settings*

Log Subscriptions

Log Name	Type	Log Files	All Rollover	Delete
antispam	Anti-Spam Logs	ftp://esa01/antispam	☐	🗑
antivirus	Anti-Virus Logs	ftp://esa01/antivirus	☐	🗑
asarchive	Anti-Spam Archive	ftp://esa01/asarchive	☐	🗑
authentication	Authentication Logs	ftp://esa01/authentication	☐	🗑
avarchive	Anti-Virus Archive	ftp://esa01/avarchive	☐	🗑
bounces	Bounce Logs	ftp://esa01/bounces	☐	🗑
cli_logs	CLI Audit Logs	ftp://esa01/cli_logs	☐	🗑
encryption	Encryption Logs	ftp://esa01/encryption	☐	🗑
error_logs	IronPort Text Mail Logs	ftp://esa01/error_logs	☐	🗑
euq_logs	IronPort Spam Quarantine Logs	ftp://esa01/euq_logs	☐	🗑
euqgui_logs	IronPort Spam Quarantine GUI Logs	ftp://esa01/euqgui_logs	☐	🗑
ftpd_logs	FTP Server Logs	ftp://esa01/ftpd_logs	☐	🗑
gui_logs	HTTP Logs	ftp://esa01/gui_logs	☐	🗑
mail_logs	IronPort Text Mail Logs	ftp://esa01/mail_logs	☐	🗑
reportd_logs	Reporting Logs	ftp://esa01/reportd_logs	☐	🗑
reportqueryd_logs	Reporting Query Logs	ftp://esa01/reportqueryd_logs	☐	🗑
scanning	Scanning Logs	ftp://esa01/scanning	☐	🗑
slbld_logs	Safe/Block Lists Logs	ftp://esa01/slbld_logs	☐	🗑
sntpd_logs	NTP logs	ftp://esa01/sntpd_logs	☐	🗑
status	Status Logs	ftp://esa01/status	☐	🗑
system_logs	System Logs	ftp://esa01/system_logs	☐	🗑
trackerd_logs	Tracking Logs	ftp://esa01/trackerd_logs	☐	🗑
updater_logs	Updater Logs	ftp://esa01/updater_logs	☐	🗑

Note: To view log files via FTP you must enable the FTP service on the 'Management' Interface.

Viewing Recent Log Entries in the CLI (tail Command)

AsyncOS supports a `tail` command, which shows the latest entries of configured logs on the appliance. Issue the `tail` command and select the number of a currently configured log to view it. Use Ctrl-C to exit from the `tail` command.

Example

In the following example, the `tail` command is used to view the system log. (This log tracks user comments from the `commit` command, among other things.) The tail command also accepts the name of a log to view as a parameter: `tail mail_logs`.

```
mail3.example.com> tail


Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll

4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll

6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll

8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll

9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll

10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP
Poll

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval:
FTP Poll

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll

13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll

14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
```

15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll

17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll

19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll

20. "status" Type: "Status Logs" Retrieval: FTP Poll

21. "system_logs" Type: "System Logs" Retrieval: FTP Poll

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll

23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

Enter the number of the log you wish to tail.

[]> **19**

Press Ctrl-C to stop.

Sat May 15 12:25:10 2008 Info: PID 274: User system commit changes: Automated Update for Quarantine Delivery Host

Sat May 15 23:18:10 2008 Info: PID 19626: User admin commit changes:

Sat May 15 23:18:10 2008 Info: PID 274: User system commit changes: Updated filter logs config

Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Receiving suspended.

^Cmail3.example.com>

Configuring Host Keys

Use the `logconfig -> hostkeyconfig` subcommand to manage host keys for use with SSH when pushing logs to other servers from the IronPort appliance. SSH servers must have a pair of host keys, one private and one public. The private host key resides on the SSH server and cannot be read by remote machines. The public host key is distributed to any client machine that needs to interact with the SSH server.

Note To manage user keys, see Managing Secure Shell (SSH) Keys, page 8-346.

The `hostkeyconfig` subcommand performs the following functions:

Table 5-35   Managing Host Keys - List of Subcommands

Command	Description
New	Add a new key.
Edit	Modify an existing key.
Delete	Delete an existing key.
Scan	Automatically download a host key.
Print	Display a key.
Host	Display system host keys. This is the value to place in the remote system's 'known_hosts' file.
Fingerprint	Display system host key fingerprints.
User	Display the public key of the system account that pushes the logs to the remote machine. This is the same key that is displayed when setting up an SCP push subscription. This is the value to place in the remote system's 'authorized_keys' file.

In the following example, AsyncOS scans for host keys and add them for the host:

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

```
Currently configured logs:

[ list of logs ]



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.

[]> hostkeyconfig



Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]



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 system host keys.
```

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]> **scan**

Please enter the host or IP address to lookup.

[]> **mail3.example.com**

Choose the ssh protocol type:

1. SSH1:rsa

2. SSH2:rsa

3. SSH2:dsa

4. All

[4]>

SSH2:dsa

mail3.example.com ssh-dss

[*key displayed*]

SSH2:rsa

mail3.example.com ssh-rsa

[*key displayed*]

```
SSH1:rsa

mail3.example.com 1024 35

[ key displayed ]


Add the preceding host key(s) for mail3.example.com? [Y]>


Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

2. mail3.example.com ssh-rsa [ key displayed ]

3. mail3.example.com 1024 35 [ key displayed ]


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 system host keys.

- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]>
```

```
Currently configured logs:

[ list of configured logs ]



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.

[]>



mail3.example.com> commit
```

Managing and Monitoring via the CLI

The Cisco IronPort appliance provides commands to allow you to monitor email operations without analyzing logs. You can monitor the Cisco IronPort appliance either via the Command Line Interface (CLI) or the Graphical User Interface (GUI). This chapter describes the monitoring and management commands and how they are accessed via the CLI. Many of the components are also available from the GUI. See Chapter 7, "Other Tasks in the GUI" for information on the GUI.

This chapter contains the following sections:

Reading the Available Components of Monitoring

Three of the key components to system monitoring:

- Counters
- Gauges
- Rates

Reading the Counters

Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime.

Counters increment each time an event occurs and are displayed in three versions:

Reset	Since the last counter reset with the `resetcounters` command
Uptime	Since the last system reboot
Lifetime	Total through the lifetime of the Cisco IronPort appliance

Table 6-1 lists the available counters and their description when monitoring the Cisco IronPort appliance.

✎

Note   This is the entire list. The displayed counters vary depending on which display option or command you choose. Use this list as a reference.

Table 6-1   Counters

Statistic	Description
Receiving	
Messages Received	Messages received into the delivery queue.
Recipients Received	Recipients on all received messages.
Generated Bounce Recipients	Recipients for which bounces have been generated by the system and inserted into the delivery queue.

Table 6-1   Counters (continued)

Statistic	Description
Rejection	
Rejected Recipients	Recipients that have been denied receiving into the delivery queue due to the Recipient Access Table (RAT), or unexpected protocol negotiation including premature connection termination.
Dropped Messages	Messages that have been denied receiving into the delivery queue due to a filter drop action match or have been received by a Black Hole queuing listener. Messages directed to `/dev/null` entries in the alias table also are considered dropped messages. Messages dropped by anti-spam filtering (if it has been enabled on the system) also increment this counter.
Queue	
Soft Bounced Events	Number of soft bounce events — a message that soft bounces multiple times has multiple soft bounce events.
Completion	
Completed Recipients	Total of all hard bounced recipients, delivered recipients, and deleted recipients. Any recipient that is removed from the delivery queue.
Hard Bounced Recipients	Total of all DNS hard bounces, 5XX hard bounces, filter hard bounces, expired hard bounces and other hard bounces. A failed attempt to deliver message to a recipient that results in immediate termination of that delivery.
DNS Hard Bounces	DNS error encountered while trying to deliver a message to a recipient.
5XX Hard Bounces	The destination mail server returned a "5XX" response code while trying to deliver a message to a recipient.

Table 6-1   Counters (continued)

Statistic	Description
Expired Hard Bounces	Message recipients that have exceeded the maximum time allowed in the delivery queue or the maximum number of connection attempts.
Filter Hard Bounces	Recipient delivery has been preempted by a matching filter bounce action. Messages dropped by anti-spam filtering (if it has been enabled on the system) also increment this counter.
Other Hard Bounces	An unexpected error during message delivery or a message recipient was explicitly bounced via the bouncerecipients command.
Delivered Recipients	Message successfully delivered to a recipient.
Deleted Recipients	Total of message recipients explicitly deleted via the deleterecipients command or was a Global Unsubscribe Hit.
Global Unsubscribe Hits	Message recipient was deleted due to a matching global unsubscribe setting.
Current IDs	
Message ID (MID)	The last Message ID to have been assigned to a message inserted into the delivery queue. A MID is associated with every message received by the Cisco IronPort appliance and can be tracked in mail logs. The MID resets to zero at 2^{31}.
Injection Connection ID (ICID)	The last Injection Connection ID to have been assigned to a connection to a listener interface. The ICID rolls over (resets to zero) at 2^{31}.
Delivery Connection ID (DCID)	The last Delivery Connection ID to have been assigned to a connection to a destination mail server. The DCID rolls over (resets to zero) at 2^{31}.

Reading the Gauges

Gauges show the current utilization of a system resource such as memory, disk space, or active connections.

Table 6-2 lists the available gauges and their description when monitoring the Cisco IronPort appliance.

Note   This is the entire list. The displayed gauges will vary depending upon which display option or command you choose. Use this list as a reference.

Table 6-2   Gauges

Statistic	Description
System Gauges	
RAM Utilization	Percentage of physical RAM (Random Access Memory) being used by the system.
CPU Utilization	Percentage of CPU usage.
Disk I/O Utilization	Percentage of Disk I/O being used. **Note** The Disk I/O Utilization gauge does not display a reading against a scale of a known value. Rather, it displays the I/O utilization the system has seen thus far and scales against the maximum value since the last reboot. So, if the gauge displays 100%, the system is experiencing the highest level of I/O utilization seen since boot (which may not necessarily represent 100% of the physical Disk I/O of the entire system).

Table 6-2   Gauges (continued)

Statistic	Description
Resource Conservation	A value between 0 and 60 or 999. Numbers from 0 to 60 represent the degree to which the system is decreasing its acceptance of messages in order to prevent the rapid depletion of critical system resources. Higher numbers represent a higher degree of decreased acceptance. Zero represents no decrease in acceptance. If this gauge displays 999, the system has entered "Resource Conservation mode," and it will accept no messages. Alert messages are sent whenever the system enters or exits Resource Conservation mode.
Disk Utilization: Logs	Percentage of disk being used for logs, displayed as LogUsd in the status logs and log_used in the XML status.

Table 6-2   Gauges (continued)

Statistic	Description
Connections Gauges	
Current Inbound Connections	Current inbound connections to the listener interfaces.
Current Outbound Connections	Current outbound connections to destination mail servers.
Queue Gauges	
Active Recipients	Message recipients in the delivery queue. Total of Unattempted Recipients and Attempted Recipients.
Unattempted Recipients	A subcategory of Active Recipients. Message recipients in queue for which delivery has not yet been attempted.
Attempted Recipients	A subcategory of Active Recipients. Message recipients in queue for which delivery has been attempted but failed due to a Soft Bounces Event.
Messages in Work Queue	The number of messages waiting to be processed by alias table expansion, masquerading, anti-spam, anti-virus scanning, message filters, and LDAP queries prior to being enqueued.
Messages in Quarantine	The unique number of messages in any quarantine, plus messages that have been released or deleted but not yet acted upon. For example, if you release all quarantined messages from Outbreak, the total messages for Outbreak would become zero immediately, but this field still reflects the quarantined messages until they were all delivered.

Table 6-2   Gauges (continued)

Statistic	Description
Destinations in Memory	The number of destinations domains in memory. For each domain with a message destined to be delivered, a destination object is created in memory. After all the mail for that domain has been delivered, the destination object is retained for another 3 hours. After 3 hours, if no new messages are bound for that domain, the object is expired so that the destination is no longer reported (for example, in the `tophosts` command). If you are delivering mail only to one domain, this counter will be "1." If you have never received or sent any messages (or no messages have been processed by the appliance in many hours), the counter will be "0."
	If you are using Virtual Gateways, destination domains for each Virtual Gateway will have a separate destination object. (For example, yahoo.com will count as 3 destination objects if you are delivering to yahoo.com from 3 different Virtual Gateways).
Kilobytes Used	Queue storage used in kilobytes.
Kilobytes in Quarantine	Queue storage used for quarantined messages. The value is calculated as the message size plus 30 bytes for each recipient, totaled for the "Messages in Quarantine" as counted above. Note that this calculation will usually *overestimate* the space used.
Kilobytes Free	Queue storage remaining in kilobytes.

Reading the Rates

All rates are shown as the average rate an event occurs per hour at the specific point in time the query is made. Rates are calculated for three intervals, the average rate per hour over the past one (1) minute, the past five (5) minutes, and the past fifteen (15) minutes.

For example, if the IronPort appliance receives 100 recipients in a single minute, then the rate for the 1 minute interval will be 6,000 per hour. The rate for the 5-minute interval will be 1,200 per hour, and the 15-minute rate will be 400 per hour. The rates are calculated to indicate what the average rate for the hour would be if the rate for the one minute period continued. Therefore, 100 messages each minute would yield a higher rate than 100 messages over 15 minutes.

Table 6-3 lists the available rates and their description when monitoring the Cisco IronPort appliance.

Note   This is the entire list. The displayed rates will vary depending upon which display option or command you choose. Use this list as a reference.

Table 6-3   Rates

Statistic	Description
Messages Received	Rate of messages inserted into the delivery queue per hour.
Recipients Received	Rate of the number of recipients on all messages inserted into the delivery queue per hour.
Soft Bounced Events	Rate of the number of soft bounce events per hour. (A message that soft bounces multiple times has multiple soft bounce events.)
Completed Recipients	Rate of the total of all hard bounced recipients, delivered recipients and deleted recipients. Any recipient that is removed from the delivery queue is considered completed.
Hard Bounced Recipients	Rate of the total of all DNS hard bounces, 5XX hard bounces, filter hard bounces, expired hard bounces and other hard bounces per hour. A failed attempt to deliver a message to a recipient that results in immediate termination of that delivery is a hard bounce.
Delivered Recipients	Rate of messages successfully delivered to a recipient per hour.

Monitoring Via the CLI

This section describes the following topics:

Monitoring the Email Status

You may want to monitor the status of email operations on the Cisco IronPort appliance. The `status` command returns a subset of the monitored information about email operations. The statistics returned displayed in one of two fashions: counters and gauges. Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime. Gauges show the current utilization of a system resource such as memory, disk space, or active connections.

For a description of each item, see Reading the Available Components of Monitoring, page 6-225.

Table 6-4   *Mail Status*

Statistic	Description
Status as of	Displays the current system time and date.
Last counter reset	Displays the last time the counters were reset.

Table 6-4   *Mail Status*

Statistic	Description
System status	Online, offline, receiving suspended, or delivery suspended. Note that the status will be "receiving suspended" only when *all* listeners are suspended. The status will be "offline" when receiving and delivery are suspended for *all* listeners.
Oldest Message	Displays the oldest message waiting to be delivered by the system.
Features	Displays any special features installed on the system by the `featurekey` command.

Example

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

```
Status as of:          Thu Oct 21 14:33:27 2004 PDT

Up since:               Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)

Last counter reset:    Never

System status:         Online

Oldest Message:         4 weeks 46 mins 53 secs


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>
```

Monitoring Detailed Email Status

The `status detail` command returns complete monitored information about email operations. The statistics returned are displayed in one of three categories: counters, rates, and gauges. Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime. Gauges show the current utilization of a system resource such as memory, disk space, or active connections. All rates are shown as the average

rate an event occurs per hour at the specific point in time the query is made. Rates are calculated for three intervals, the average rate per hour over the past one (1) minute, the past five (5) minutes, and the past fifteen (15) minutes. For a description of each item, see Reading the Available Components of Monitoring, page 6-225.

Example

```
mail3.example.com> status detail
```

```
Status as of:          Thu Jun 30 13:09:18 2005 PDT

Up since:              Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)

Last counter reset:         Tue Jun 29 19:30:42 2004 PDT

System status:              Online

Oldest Message:             No Messages

Feature - IronPort Anti-Spam:  17 days

Feature - Sophos:           Dormant/Perpetual

Feature - Virus Outbreak Filters: Dormant/Perpetual

Feature - Central Mgmt:         Dormant/Perpetual


Counters:                   Reset         Uptime        Lifetime

  Receiving

    Messages Received       2,571,967     24,760        3,113,176

    Recipients Received     2,914,875     25,450        3,468,024

    Gen. Bounce Recipients      2,165         0             7,451

  Rejection

    Rejected Recipients     1,019,453       792         1,740,603

    Dropped Messages        1,209,001        66         1,209,028

  Queue
```

```
       Soft Bounced Events      11,236              0            11,405

    Completion

      Completed Recipients    2,591,740          49,095        3,145,002

        Hard Bounced Recipients   2,469              0             7,875

          DNS Hard Bounces         199              0             3,235

          5XX Hard Bounces       2,151              0             4,520

          Expired Hard Bounces     119              0               120

          Filter Hard Bounces        0              0                 0

          Other Hard Bounces         0              0                 0

        Delivered Recipients   2,589,270          49,095        3,137,126

        Deleted Recipients           1              0                 1

        Global Unsub. Hits           0              0                 0

      DomainKeys Signed Msgs        10              9                10



    Current IDs

      Message ID (MID)                                            7615199

      Injection Conn. ID (ICID)                                   3263654

      Delivery Conn. ID (DCID)                                    1988479



    Rates (Events Per Hour):      1-Minute       5-Minutes      15-Minutes

      Receiving

      Messages Received            180             300               188
```

```
     Recipients Received        180            300            188

  Queue

    Soft Bounced Events          0              0              0

  Completion

    Completed Recipients       360            600            368

      Hard Bounced Recipients    0              0              0

      Delivered Recipients     360            600            368


  Gauges:                     Current

    System

      RAM Utilization            1%

      CPU Utilization

        MGA                      0%

        AntiSpam                 0%

        AntiVirus                0%

      Disk I/O Utilization       0%

      Resource Conservation      0

    Connections

      Current Inbound Conn.      0

      Current Outbound Conn.     0

    Queue

      Active Recipients          0
```

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

```
                  Unattempted Recipients              0

                   Attempted Recipients               0

              Messages In Work Queue                  0

              Messages In Quarantine                 19

              Destinations In Memory                  3

              Kilobytes Used                        473

                Kilobytes In Quarantine             473

              Kilobytes Free                  39,845,415
```

Note   A case could exist in a newly installed appliance where the oldest message counter shows a message but, in fact, there are no recipients shown in counters. If the remote host is connecting and in the process of receiving a message very slowly (that is, it takes minutes to receive a message), you might see that the recipients received counter displays "0" but the oldest message counter displays "1." This is because the oldest message counter displays messages in progress. The counter will be reset if the connection is eventually dropped.

Monitoring the Status of a Mail Host

If you suspect delivery problems to a specific recipient host or you want to gather information on a Virtual Gateway address, the hoststatus command displays this information. The hoststatus command returns monitoring information about email operations relating to a specific recipient host. The command requires that you enter the domain of the host information to be returned. DNS information stored in the AsyncOS cache and the last error returned from the recipient host is also given. Data returned is cumulative since the last resetcounters command. The statistics returned are displayed in two categories: counters and gauges. For a description of each item, see Reading the Available Components of Monitoring, page 6-225.

In addition, these other data are returned specific to the `hoststatus` command.

Table 6-5   *Additional Data in the hoststatus Command*

Statistic	Description
Pending Outbound Connections	Pending, or "embryonic" connections to the destination mail host, as opposed to open and working connections. Pending Outbound Connections are connections which have not yet gotten to the protocol greeting stage.
Oldest Message	The age of the oldest active recipient in the delivery queue for this domains. This counter is useful for determining the age of a message in the queue that cannot be delivered because of soft bounce events and/or a downed host.
Last Activity	This field is updated each time a message delivery is attempted to that host.
Ordered IP Addresses	This field contains the TTL (time to live) for IP addresses, their preference according to MX records, and the actual addresses. An MX record designates the mail server IP address for a domain. A domain may have multiple MX records. Each MX record mail server is assigned a priority. The MX record with the lowest priority number is given preference.
Last 5XX error	This field contains the most recent "5XX" status code and description returned by the host. This is only displayed if there is an 5XX error.
MX Records	An MX record designates the mail server IP address for a domain. A domain may have multiple MX records. Each MX record mail server is assigned a priority. The MX record with the lowest priority number is given preference.
SMTP Routes for this host	If SMTP routes are defined for this domain, they are listed here.
Last TLS Error	This field contains a description of the the most recent outgoing TLS connection error and the type of TLS connection that the appliance tried to establish. This is only displayed if there is a TLS error.

Virtual Gateway

The following Virtual Gateway information is only displayed if you have set up Virtual Gateway addresses (see "Configuring the Gateway to Receive Email" in the *Cisco IronPort AsyncOS for Email Configuration Guide*).

Table 6-6   Additional Virtual Gateway Data in the hoststatus Command

Statistic	Description
Host up/down	Same definition as global `hoststatus` field of the same name — tracked per Virtual Gateway address.
Last Activity	Same definition as global `hoststatus` field of the same name — tracked per Virtual Gateway address.
Recipients	This field also corresponds to the same definition as the global `hoststatus` command. Active Recipients field — tracked per Virtual Gateway address.
Last 5XX error	This field contains the most recent 5XX status code and description returned by the host. This is only displayed if there is a 5XX error.

Example

```
mail3.example.com> hoststatus


Recipient host:

[]> aol.com


Host mail status for: 'aol.com'

Status as of:          Tue Mar 02 15:17:32 2010

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        Tue Mar 02 15:17:32 2010

Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)

    Preference   IPs

    15           64.12.137.121   64.12.138.89    64.12.138.120

    15           64.12.137.89    64.12.138.152   152.163.224.122

    15           64.12.137.184   64.12.137.89    64.12.136.57

    15           64.12.138.57    64.12.136.153   205.188.156.122

    15           64.12.138.57    64.12.137.152   64.12.136.89

    15           64.12.138.89    205.188.156.154 64.12.138.152

    15           64.12.136.121   152.163.224.26  64.12.137.184
```

```
      15            64.12.138.120    64.12.137.152    64.12.137.121



MX Records:

    Preference    TTL         Hostname

    15            52m24s      mailin-01.mx.aol.com

    15            52m24s      mailin-02.mx.aol.com

    15            52m24s      mailin-03.mx.aol.com

    15            52m24s      mailin-04.mx.aol.com



    Last 5XX Error:

    ----------

    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE

   (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10

    ----------



    Last TLS Error:          Required - Verify

        ----------

        TLS required, STARTTLS unavailable

        (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10



Virtual gateway information:

==============================================================
```

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

```
example.com (PublicNet_017):

    Host up/down:          up

    Last Activity          Wed June 22 13:47:02 2005

    Recipients             0
```

Note   The Virtual Gateway address information only appears if you are using the
altsrchost feature.

Determining the Make-up of the Email Queue

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. For a description of each item, see Reading
the Available Components of Monitoring, page 6-225.

Example

```
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>
```

Displaying Real-time Activity

The Cisco IronPort appliance offers real-time monitoring, which allows you to view the progress of email activity on the system. The `rate` command returns real-time monitoring information about email operations. The information is updated on a periodic interval as specified by you. Use Control-C to stop the `rate` command.

The data shown are listed in Table 6-7

Table 6-7   *Data in the rate Command*

Statistic	Description
Connections In	Number of inbound connections.
Connections Out	Number of outbound connections.
Recipients Received	Total number of recipients received into the system.
Recipients Completed	Total number of recipients completed.
Delta	The difference change in Received and Completed recipients since the last data update.
Queue Used	Size of the message queue in kilobytes.

Example

```
mail3.example.com> rate


Enter the number of seconds between displays.

[10]> 1


Hit Ctrl-C to return to the main prompt.


Time     Connections Recipients        Recipients              Queue

            In   Out   Received    Delta  Completed    Delta    K-Used

23:37:13   10    2    41708833        0   40842686        0       64

23:37:14    8    2    41708841        8   40842692        6      105

23:37:15    9    2    41708848        7   40842700        8       76

23:37:16    7    3    41708852        4   40842705        5       64

23:37:17    5    3    41708858        6   40842711        6       64

23:37:18    9    3    41708871       13   40842722       11       67

23:37:19    7    3    41708881       10   40842734       12       64

23:37:21   11    3    41708893       12   40842744       10       79

^C
```

The hostrate command returns real-time monitoring information about a specific
mail host. This information is a subset of the status detail command. (See
Monitoring Detailed Email Status, page 6-237.)

Table 6-8   Data in the hostrate Command

Statistic	Description
Host Status	Current status of the specific host: up, down, or unknown.
Current Connections Out	Current number of outbound connections to the host.
Active Recipients in Queue	Total number of active recipients to the specific host in queue.
Active Recipients in Queue Delta	Difference in the total number of active recipients to the specific host in queue since the last known host status.
Delivered Recipients Delta	Difference in the total number of delivered recipients to the specific host in queue since the last known host status.
Hard Bounced Recipients Delta	Difference in the total number of hard bounced recipients to the specific host in queue since the last known host status.
Soft Bounce Events Delta	Difference in the total number of soft bounced recipients to the specific host in queue since the last known host status.

Use Control-C to stop the `hostrate` command.

Example

```
mail3.example.com> hostrate


Recipient host:

[]> aol.com


Enter the number of seconds between displays.

[10]> 1
```

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

```
^C
```

Monitoring Inbound Email Connections

You may want to monitor hosts that are connecting to the Cisco IronPort appliance to identify the large volume senders or to troubleshoot inbound connections to the system. The `topin` command provides a snapshot of the remote hosts connecting to the system. It displays a table with one row for each remote IP address

connecting to a specific listener. Two connections from the same IP address to different listeners results in 2 rows in the table. Table 6-9 describes the fields displayed when using the topin command.

Table 6-9   Data in the topin Command

Statistic	Description
Remote Hostname	Hostname of the remote host, derived from Reverse DNS lookup.
Remote IP Address	IP address of the remote host.
listener	Nickname of the listener on the Cisco IronPort appliance that is receiving the connection.
Connections In	The number of concurrent connections from the remote host with the specified IP address open at the time when the command is run.

The system does a reverse DNS lookup to find the remote hostname, and then a forward DNS lookup to validate the name. If the forward lookup does not result in the original IP address, or if the reverse DNS lookup fails, the table displays the IP address in the hostname column. For more information about the process of sender verification, see "Sender Verification" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Example

```
mail3.example.com> topin



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



#  Remote hostname          Remote IP addr.   listener      Conn. In

1  mail.remotedomain01.com  172.16.0.2        Incoming01          10
```

```
2  mail.remotedomain01.com    172.16.0.2     Incoming02           10

3  mail.remotedomain03.com    172.16.0.4     Incoming01            5

4  mail.remotedomain04.com    172.16.0.5     Incoming02            4

5  mail.remotedomain05.com    172.16.0.6     Incoming01            3


6  mail.remotedomain06.com    172.16.0.7     Incoming02            3

7  mail.remotedomain07.com    172.16.0.8     Incoming01            3

8  mail.remotedomain08.com    172.16.0.9     Incoming01            3

9  mail.remotedomain09.com    172.16.0.10    Incoming01            3

10 mail.remotedomain10.com    172.16.0.11    Incoming01            2


11 mail.remotedomain11.com    172.16.0.12    Incoming01            2

12 mail.remotedomain12.com    172.16.0.13    Incoming02            2

13 mail.remotedomain13.com    172.16.0.14    Incoming01            2

14 mail.remotedomain14.com    172.16.0.15    Incoming01            2

15 mail.remotedomain15.com    172.16.0.16    Incoming01            2


16 mail.remotedomain16.com    172.16.0.17    Incoming01            2

17 mail.remotedomain17.com    172.16.0.18    Incoming01            1

18 mail.remotedomain18.com    172.16.0.19    Incoming02            1

19 mail.remotedomain19.com    172.16.0.20    Incoming01            1

20 mail.remotedomain20.com    172.16.0.21    Incoming01            1
```

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

Checking the DNS Status

The `dnsstatus` command returns a counter displaying statistics of DNS lookup and cache information. For each counter, you can view the total number of events since the counter was last reset, since the last system reboot, and over the lifetime of the system.

Table 6-10 lists the available counters.

Table 6-10   Data in the dnsstatus Command

Statistic	Description
DNS Requests	A top-level, non-recursive request to the system DNS cache to resolve a domain name.
Network Requests	A request to the network (non-local) to retrieve DNS information.
Cache Hits	A request to the DNS cache where the record was found and returned.
Cache Misses	A request to the DNS cache where the record was not found.
Cache Exceptions	A request to the DNS cache where the record was found but the domain was unknown.
Cache Expired	A request to the DNS cache where the record was found in the cache, considered for use, and discarded because it was too old. Many entries can exist in the cache even though their time to live (TTL) has been exceeded. As long as these entries are not used, they will not be included in the expires counter. When the cache is flushed, both valid and invalid (too old) entries are deleted. A flush operation does not change the expires counter.

Example

```
mail3.example.com> dnsstatus


Status as of: Sat Aug 23 21:57:28 2003


Counters:                    Reset          Uptime          Lifetime

  DNS Requests         211,735,710       8,269,306       252,177,342

  Network Requests     182,026,818       6,858,332       206,963,542

  Cache Hits           474,675,247      17,934,227       541,605,545

  Cache Misses         624,023,089      24,072,819       704,767,877

  Cache Exceptions      35,246,211       1,568,005        51,445,744

  Cache Expired            418,369           7,800           429,015


mail3.example.com>
```

Resetting Email Monitoring Counters

The resetcounters command resets cumulative email monitoring counters. The reset affects global counters as well as per host counters. The reset does not affect the counters on messages in the delivery queue related to retry schedules.

Note   You can also reset the counters in the GUI. See The System Status Page, page 2-64.

Example

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

```
Counters reset: Mon Jan 01 12:00:01 2003
```

Managing the Email Queue

IronPort AsyncOS allows you to perform operations on messages in the email queue. You can delete, bounce, suspend, or redirect messages in the email queue. You can also locate, remove, and archive older messages in your queue.

Deleting Recipients in Queue

If particular recipients are not being delivered or to clear the email queue, use the deleterecipients command. The deleterecipients command allows you to manage the email delivery queue by deleting specific recipients waiting for delivery. Recipients to be deleted are identified by either the recipient host that the recipient is destined for, or the message sender identified by the specific address given in the Envelope From line of the message envelope. Alternately, you can delete all messages in the delivery queue (all active recipients) at once.

> **Note** To perform the deleterecipients function, it is recommended that you place the IronPort appliance in an offline state or suspended delivery (see Placing the IronPort Appliance into a Maintenance State, page 8-309).

> **Note** Although the function is supported in all states, certain messages may be delivered while the function is taking place.

Matches to recipient hosts and senders must be identical string matches. Wild cards are not accepted. The `deleterecipients` command returns the total number of messages deleted. In addition, if a mail log subscription (IronPort text format only) is configured, the message deletion is logged as a separate line.

Example

```
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]>
```

The Cisco 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

```
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

```
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

```
Are you sure you want to delete all messages in the delivery queue (all
active recipients)? [N]> Y



Deleting messages, please wait.

1000 messages deleted.
```

Bouncing Recipients in Queue

Similar to the deleterecipients command, the bouncerecipients command allows you to manage the email delivery queue by hard bouncing specific recipients waiting for delivery. Message bouncing follows regular bounce message configuration as specified in the bounceconfig command.

Note   To perform the bouncerecipients function, it is recommended that you place the IronPort appliance in an offline state or suspended delivery (see Placing the IronPort Appliance into a Maintenance State, page 8-309).

Note   Although the function is supported in all states, certain messages may be delivered while the function is taking place.

Matches to recipient hosts and senders must be identical string matches. Wild cards are not accepted. The bouncerecipients command returns the total number of messages bounced.

Note   The bouncerecipients function is resource-intensive and may take several minutes to complete. If in offline or suspended delivery state, the actual sending of bounce messages (if hard bounce generation is on) will begin only after IronPort AsyncOS is placed back into the online state by using the resume command.

Example

```
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]>
```

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

```
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

```
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

```
Are you sure you want to bounce all messages in the queue? [N]> Y
```

```
Bouncing messages, please wait.

1000 messages bounced.
```

Suspending Email Delivery

To temporarily suspend email delivery for maintenance or troubleshooting, use the `suspenddel` command. The `suspenddel` command puts IronPort AsyncOS into suspended delivery state. This state is characterized by the following:

- Outbound email delivery is halted.

- Inbound email connections are accepted.

- Log transfers continue.

- The CLI remains accessible.

The `suspenddel` command lets open outbound connections close, and it stops any new connections from opening. The `suspenddel` command commences immediately, and allows any established connections to successfully close. Use the `resumedel` command to return to regular operations from the suspended delivery state.

![Note icon]

Note   The "delivery suspend" state is preserved across system reboots. If you use the `suspenddel` command and then reboot the appliance, you must resume delivery after the reboot using the `resumedel` command.

Example

```
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.
```

Resuming Email Delivery

The resumedel command returns IronPort AsyncOS to normal operating state after using the suspenddel command.

Syntax

```
        resumedel

mail3.example.com> resumedel



Mail delivery resumed.
```

Suspending Receiving

To temporarily suspend all listeners from receiving email, use the suspendlistener command. While receiving is suspended, the system does not accept connections to the specific port of the listener.

This behavior has changed in this release of AsyncOS. In previous releases, the system would accept connections, respond with the following responses and disconnect:

- SMTP: 421 *hostname* `Service not available, closing transaction channel`

- QMQP: `ZService not available`

Note The "receiving suspend" state is preserved across system reboots. If you use the `suspendlistener` command and then reboot the appliance, you must use the `resumelistener` command before the listener will resume receiving messages.

Syntax

```
        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>
```

Resuming Receiving

The `resumedlistener` command returns IronPort AsyncOS to normal operating state after using the `suspendlistener` command.

Syntax

```
        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>
```

Resuming Delivery and Receiving

The resume command resumes both delivery and receiving.

Syntax

```
        resume

mail3.example.com> resume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

Scheduling Email for Immediate Delivery

Recipients and hosts that are scheduled for later delivery can be immediately retried by using the `delivernow` command. The `delivernow` command allows you to reschedule email in the queue for immediate delivery. All domains that are marked down and any scheduled or soft bounced messages are queued for immediate delivery.

The `delivernow` command can be invoked for all recipients or specific recipients in the queue (scheduled and active). When selecting specific recipients, you must enter the domain name of the recipients to schedule for immediate delivery. The system matches the entire string for character and length.

Syntax

```
        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.
```

```
[]> recipient.example.com
```

```
Rescheduling all messages to recipient.example.com for immediate
delivery.
```

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

Pausing the Work Queue

Processing for LDAP recipient access, masquerading, LDAP re-routing, Message Filters, anti-spam, and the anti-virus scanning engine are all performed in the "work queue." Refer to "Configuring Routing and Delivery Features" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide* for the processing flow and for a description of the "Messages in Work Queue" gauge. You can manually pause the work queue portion of message processing using the workqueue command.

For example, assume that you wanted to change the configuration of an LDAP server configuration while many messages are in the work queue. Perhaps you want to switch from bouncing to dropping messages based on an LDAP recipient access query. Or perhaps you want to pause the queue while you manually check for the latest anti-virus scanning engine definition files (via the antivirusupdate command).The workqueue command allows you to pause and resume the work queue to stop processing while you perform other configuration changes.

When you pause and resume the work queue, the event is logged. For example

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S

Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

In the following example, the work queue is paused:

```
mail3.example.com> workqueue


Status as of:  Sun Aug 17 20:02:30 2003 GMT

Status:   Operational

Messages: 1243


Choose the operation you want to perform:

- STATUS - Display work queue status

- PAUSE - Pause the work queue

- RATE - Display work queue statistics over time

[]> pause


Manually pause work queue?  This will only affect unprocessed messages.
[N]> y


Reason for pausing work queue:

[]> checking LDAP server


Status as of:  Sun Aug 17 20:04:21 2003 GMT

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 "`Manually paused by user.`"

In this example, the work queue is resumed:

```
mail3.example.com> workqueue



Status as of:  Sun Aug 17 20:42:10 2003 GMT

Status:   Paused by admin: checking LDAP server

Messages: 1243



Choose the operation you want to perform:

- STATUS - Display work queue status

- RESUME - Resume the work queue

- RATE - Display work queue statistics over time

[]> resume



Status:   Operational

Messages: 1243
```

Locating and Archiving Older Messages

Sometimes older messages remain in the queue because they could not be
delivered. You may want to remove and archive these messages. To do this, use
the showmessage CLI command to to display the message for the given message
ID. Use the oldmessage CLI command to display the oldest non-quarantine

message on the system. You can then optionally use the `removemessage` to safely remove the message for the given message ID. This command can only remove messages that are in the work queue, retry queue, or a destination queue. If the message is in none of these queues, it cannot be removed.

You can also use the `archivemessage[mid]` CLI command to archive the message for a given message ID into an mbox file in the configuration directory.

You cannot use the `oldmessage` command to get the message ID for a message in a system quarantine. However, if you know the message ID, you can show or archive the specified message. Since the message is not in the work queue, retry queue, or a destination queue, you cannot remove the message with the `removemessage` command.

Note You cannot perform any of these queue management commands on a message in the IronPort Spam Quarantine.

Syntax

```
archivemessage

example.com> archivemessage


Enter the MID to archive and remove.

[0]> 47

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

example.com>
```

Syntax

```
oldmessage

example.com> oldmessage
```

```
MID 9: 1 hour 5 mins 35 secs old

Received: from example.com ([172.16.0.102])

  by example.com with SMTP; 14 Feb 2007 22:11:37 -0800

From: user123@example.com

To: 4031@test.example2.com

Subject: Testing

Message-Id: <20070215061136.68297.16346@example.com>
```

Tracking Messages Within the System

The findevent CLI command simplifies the process of tracking messages within the system using the onbox mail log files. The findevent CLI command allows you to search through the mail logs for a particular message by searching for a message ID or a regular expression match against the subject header, envelope sender or envelope recipient. You can display results for the current log file, all the log files, or display log files by date. When you view log files by date, you can specify a date or a range of dates.

After you identify the message you want to view logs for, the findevent command displays the log information for that message ID including splintering information (split log messages, bounces and system generated messages). The following example shows the findevent CLI command tracking the receiving and delivery a message with "confidential" in the subject header:

```
example.com> findevent

Please choose which type of search you want to perform:

1. Search by envelope FROM

2. Search by Message ID
```

```
3. Search by Subject

4. Search by envelope TO

[1]> 3

Enter the regular expression to search for.

[]> confidential

Currently configured logs:

1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll

Enter the number of the log you wish to use for message tracking.

[]> 1

Please choose which set of logs to search:

1. All available log files

2. Select log files by date list

3. Current log file
```

```
[3]> 3

The following matching message IDs were found. Please choose one to
show additional log information:
1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential
[1]> 1
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1
(172.19.1.86) address 10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To:
<ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from
<user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for
per-recipient policy DEFAULT in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE
spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos
CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

SNMP Monitoring

The IronPort AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). This includes IronPort's Enterprise MIB, ASYNCOS-MAIL-MIB. The ASYNCOS-MAIL-MIB helps administrators better monitor system health. In addition, this release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907. (For more information on SNMP, see RFCs 1065, 1066, and 1067.) Please note:

- SNMP is **off** by default.

- SNMP SET operations (configuration) are not implemented.

- AsyncOS supports SNMPv1, v2, and v3.

- The use of SNMPv3 with password authentication and DES Encryption is mandatory to enable this service. (For more information on SNMPv3, see RFCs 2571-2575.) You are required to set a SNMPv3 passphrase of at least 8 characters to enable SNMP system status monitoring. The first time you enter a SNMPv3 passphrase, you must re-enter it to confirm. The `snmpconfig` command "remembers" this phrase the next time you run the command.

- The SNMPv3 username is: v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
```

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to `public`.

- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.

- To use traps, an SNMP manager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a hostname, but if you do, traps will only work if DNS is working.)

Use the `snmpconfig` command to configure SNMP system status for the appliance. After you choose and configure values for an interface, the appliance responds to SNMPv3 GET requests. These version 3 requests must include a matching password. By default, version 1 and 2 requests are rejected. If enabled, version 1 and 2 requests must have a matching community string.

MIB Files

IronPort Systems provides an "enterprise" MIB as well as a "Structure of Management Information" (SMI) file:

- ASYNCOS-MAIL-MIB.txt — an SNMPv2 compatible description of the Enterprise MIB for IronPort appliances.

- IRONPORT-SMI.txt — defines the role of the ASYNCOS-MAIL-MIB in IronPort's SNMP managed products.

These files are available on the documentation CD included with your Cisco IronPort appliance. You can also request these files through IronPort Customer Support.

Hardware Objects

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report temperature, fan speed, and power supply status.

Table 6-11 shows what hardware derived objects are available for monitoring on what models. The number displayed is the number of instances of that object that can be monitored. For example, you can query the RPMs for 3 fans in the C10 appliance and 6 fans in the C300/C600/X1000 appliances.

Table 6-11   Number of Hardware Objects per IronPort Appliance

Model	CPU Temp	Ambient Temp	Backplane Temp	Riser Temp	Fans	Power Supply Status	Disk Status	NIC Link
C10/100	1	1	0	0	3	0	2	2
C30/C60	0	0	0	0	0	0	2 (C60 has 4)	3
C300/C600 /X1000	2	1	1	1	6	2	4 (C300 has 2)	3 (*5 for C600 and X1000 with fiber interface*)
C350/C650 /X1050	2	1	0	0	4	2	4 (C350 has 2)	3 (*5 for the C650 and x1050 with fiber interface*)

All models can use SNMP to monitor disk drive health and the link status of Network Interfaces.

Hardware Traps

Table 6-12 lists the temperature and hardware conditions that cause a hardware trap to be sent:

Table 6-12   *Hardware Traps: Temperature and Hardware Conditions*

Model	High Temp (CPU)	High Temp (Ambient)	High Temp (Backplane)	High Temp (Riser)	Fan Failure	Power Supply	RAID	Link
C10/C100	90C	47C	NA	NA	0 RPMs	Status Change	Status Change	Status Change
C30/C60	NA	NA	NA	NA	NA	NA	Status Change	Status Change
C300/C600/X1000	90C	47C	72C	62C	0 RPMs	Status Change	Status Change	Status Change
C350/C650/X1050	90C	47C	NA	NA	0 RPMs	Status Change	Status Change	Status Change

Status change traps are sent when the status changes. Fan Failure and high temperature traps are sent every 5 seconds. The other traps are failure condition alarm traps — they are sent once when the state changes (healthy to failure). It is a good idea to poll for the hardware status tables and identify possible hardware failures before they become critical. Temperatures within 10 per cent of the critical value may be a cause for concern.

Note that failure condition alarm traps represent a critical failure of the individual component, but may not cause a total system failure. For example, a single fan or power supply can fail on a C600 appliance and the appliance will continue to operate.

SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application (an SNMP management console, typically) when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. Traps are generated when a condition has been met on the SNMP agent (in this case, the Cisco IronPort

appliance). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it over port 162, the standard SNMP trap port. In the example below, the trap target of snmp-monitor.example.com and the Trap Community string are entered. This is the host running the SNMP management console software that will receive the SNMP traps from the IronPort appliance.

You can configure SNMP traps (enable or disable specific traps) when you enable SNMP for an interface. To specify multiple trap targets: when prompted for the trap target, you may enter up to 10 comma separated IP addresses.

CLI Example

In the following example, the snmpconfig command is used to enable SNMP on the "PublicNet" interface on port 161. A passphrase for version 3 is entered and then re-entered for confirmation. The system is configured to service version 1 and 2 requests, and the community string public is entered for GET requests from those versions 1 and 2. The trap target of snmp-monitor.example.com is entered. Finally, system location and contact information is entered.

```
mail3.example.com> snmpconfig



Current SNMP settings:

SNMP Disabled.



Choose the operation you want to perform:

- SETUP - Configure SNMP.

[]> setup



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



Please choose an IP interface for SNMP requests.
```

■ **SNMP Monitoring**

```
1. Data 1 (192.168.1.1/24: mail3.example.com)

2. Data 2 (192.168.2.1/24: mail3.example.com)

3. Management (192.168.44.44/24: mail3.example.com)

[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 recommended). Enter "None" to disable
traps.
```

```
[None]> 10.1.1.29


Enter the Trap Community string.

[]> tcomm


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
```

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

```
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: 10.1.1.29

Location: Network Operations Center - west; rack #31, position 2

System Contact: Joe Administrator, x8888


mail3.example.com>
```

Other Tasks in the GUI

The graphical user interface (GUI) is the web-based alternative to some command line interface (CLI) commands for system monitoring and configuration. The GUI enables you to monitor the system using a simple Web-based interface without having to learn the IronPort AsyncOS command syntax.

This chapter contains the following sections:

The Cisco IronPort Graphical User Interface (GUI)

After HTTP and/or HTTPS services have been enabled for an interface, you can access the GUI and log in. See the "Overview" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Enabling the GUI on an Interface

By default, the system ships with HTTP enabled on the Management interface (Data 1 for IronPort C10/100 appliances).

To enable the GUI, execute the `interfaceconfig` command at the command-line interface, edit the interface that you want to connect to, and then enable the HTTP services or secure HTTP services, or both.

Note   You can also use the Network > IP Interfaces page to enable or disable the GUI on an interface, once you have the GUI enabled on any other interface. See IP Interfaces, page -294 for more information.

Note   Enabling secure HTTP on an interface requires you to install a certificate. For more information, see "Enabling a Certificate for HTTPS" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

For either service, you specify the port on which you want the service to be enabled. By default, HTTP is enabled on port 80 and HTTPS on port 443. If you enable both services for an interface, you can automatically redirect HTTP requests to the secure service.

In addition, all users (see Adding Users, page 8-324) who attempt to access the GUI on this interface (either via HTTP or HTTPS) must authenticate themselves via a standard username and password login page.

Note   You must save the changes by using the commit command before you are able to access the GUI.

In the following example, the GUI is enabled for the Data 1 interface. The interfaceconfig command is used to enable HTTP on port 80 and HTTPS on port 443. (The demonstration certificate is temporarily used for HTTP until the certconfig command can be run. For more information, see "Installing Certificates on the Cisco IronPort Appliance" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.) HTTP requests to port 80 are configured to be automatically redirected to port 443 for the Data1 interface.

Example

```
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?

[80]> 80



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



Which port do you want to use for HTTPS?

[443]> 443



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?  [N]> y



Both HTTP and HTTPS are enabled for this interface, should HTTP
requests

redirect to the secure service?  [Y]> 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>
```

Overview of Remaining Tasks Available in the GUI

- On the **System Overview** page, you can:
    - View historical graphs and tables showing some of the key system status and performance information.
    - View the version of the IronPort AsyncOS operating system installed on the appliance.
    - View a subset of key statistics.
- The **System Status** page provides a detailed representation of all real-time mail and DNS activity for the system. You can also reset the counters for system statistics and view the last time the counters were reset.

- On the **System Trace** page, you can debug the flow of messages through the system by emulating sending a test message. You can emulate a message as being accepted by a listener and print a summary of features that would have been "triggered" or affected by the current configuration of the system.

Debugging Mail Flow Using Test Messages: Trace

You can use System Administration > Trace page (the equivalent of the `trace` command in the CLI) to debug the flow of messages through the system by emulating sending a test message. The Trace page (and `trace` CLI command) emulates a message as being accepted by a listener and prints a summary of features that would have been "triggered" or affected by the current configuration (*including uncommitted changes*) of the system. The test message is not actually sent. The Trace page (and `trace` CLI command) can be a powerful troubleshooting or debugging tool, especially if you have combined many of the advanced features available on the Cisco IronPort appliance.

The Trace page (and `trace` CLI command) prompts you for the input parameters listed in Table 7-1.

Table 7-1   Input for the Trace page

Value	Description	Example
Source IP address	Type the IP address of the remote client to mimic the source of the remote domain. **Note:** The `trace` command prompts for an IP address and a fully-qualified domain name. It does *not* attempt to reverse the IP address to see if it matches the fully-qualified domain name. The `trace` command does not allow the fully-qualified domain name field to be blank, so it is impossible to test a scenario where the DNS does not reverse match properly.	`203.45.98.109`
Fully Qualified Domain Name of the Source IP	Type the fully-qualified remote domain name to mimic. If left null, a reverse DNS lookup will be performed on the source IP address.	`smtp.example.com`
Listener to Trace Behavior on	Choose from the list of listeners configured on the system to emulate sending the test message to.	`InboundMail`
SenderBase Network Owner Organization ID	Type the unique identification number of the SenderBase network owner, or allow the system to Lookup network owner ID associated with source IP address. You can view this information if you added network owners to sender groups via the GUI.	`34`

Table 7-1   Input for the Trace page (continued)

Value	Description	Example
SenderBase Reputation Score (SBRS scores)	Type the SBRS score you want to provide for the spoofed domain, or allow the system to look up the SBRS score associated with source IP address. This can be helpful when testing policies that use SBRS scores. Note that manually entered SBRS scores are not passed to the Context Adaptive Scanning Engine (CASE). See "Reputation Filtering" in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.	`-7.5`
Envelope Sender	Type the Envelope Sender of the test message.	`admin@example.net`
Envelope Recipients	Type a list of recipients for the test message. Separate multiple entries with commas.	`joe` `frank@example.com`
Message Body	Type the message body for the test message, including headers. Type a period on a separate line to end entering the message body. Note that "headers" are considered part of a message body (separated by a blank line), and omitting headers, or including poorly formatted ones can cause unexpected trace results.	`To: 1@example.com` From: ralph Subject: Test `A test message` `.`

After you have entered the values, click **Start Trace**. A summary of all features configured on the system affecting the message is printed.

You can upload message bodies from your local file system. (In the CLI, you can test with message bodies you have uploaded to the `/configuration` directory. See Appendix A, "Accessing the Appliance" for more information on placing files for import onto the Cisco IronPort appliance.)

After the summary is printed, you are prompted to view the resulting message and re-run the test message again. If you enter another test message, the Trace page and the `trace` command uses any previous values from Table 7-1 you entered.

Note   The sections of configuration tested by the `trace` command listed in Table 7-2 are performed *in order*. This can be extremely helpful in understanding how the configuration of one feature affects another. For example, a recipient address transformed by the domain map feature will affect the address as it is evaluated by the RAT. A recipient that is affected by the RAT will affect the address as it is evaluated by alias table, and so on.

Table 7-2   Viewing Output After Performing a Trace

trace Command Section	Output
Host Access Table (HAT) and Mail Flow Policy Processing	The Host Access Table settings for the listener you specified are processed. The system reports which entry in the HAT matched from the remote IP address and remote domain name you entered. You can see the default mail flow policies and sender groups and which one matched the given entries. If the Cisco IronPort appliance was configured to reject the connection (either through a REJECT or TCPREFUSE access rule), the `trace` command exits at the point in the processing. For more information on setting HAT parameters, see "Configuring the Gateway to Receive Email" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Envelope Sender Address Processing

These sections summarize how the appliance configuration affects the Envelope Sender you supply. (That is, how the MAIL FROM command would be interpreted by the configuration of the appliance.) The `trace` command prints "`Processing MAIL FROM:`" before this section.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Default Domain	If you specified that a listener to change the default sender domain of messages it receives, any change to the Envelope Sender is printed in this section. For more information, see "SMTP Address Parsing Options" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Masquerading	If you specified that the Envelope Sender of a message should be transformed, the change is noted here. You enable masquerading for the Envelope Sender on private listeners using the `listenerconfig -> edit -> masquerade -> config` subcommands. For more information, see "Configuring Masquerading" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Envelope Recipient Processing

These sections summarize how the appliance affects the Envelope Recipients you supply. (That is, how the RCPT TO command would be interpreted by the configuration of the appliance.) The `trace` command prints "`Processing Recipient List:`" before this section.

Default Domain	If you specified that a listener to change the default sender domain of messages it receives, any changes to the Envelope Recipients are printed in this section. For more information, see "SMTP Address Parsing Options" in the "Customizing Listeners" chapter of the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Domain Map Translation	The domain map feature transforms the recipient address to an alternate address. If you specified any domain map changes and a recipient address you specified matches, the transformation is printed in this section. For more information, see "The Domain Map Feature" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Recipient Access Table (RAT)	Each Envelope Recipient that matches an entry in the RAT is printed in this section, in addition to the policy and parameters. (For example, if a recipient was specified to bypass limits in the listener's RAT.) For more information on specifying recipients you accept, see "Accepting Email for Local Domains or Specific Users on Public listeners (RAT)" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.
Alias Table	Each Envelope Recipient that matches an entry in the alias tables configured on the appliance (and the subsequent transformation to one or more recipient addresses) is printed in this section. For more information, see "Creating Alias Tables" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Pre-Queue Message Operations	
These sections summarize how the appliance affects each message after the message contents have been received, but before the messages are enqueued on the work queue. This processing occurs before the final `250 ok` command is returned to the remote MTA. The `trace` command prints "Message Processing:" before this section.	
Virtual Gateways	The `altsrchost` command assigns messages to a specific interface, based on a match of the Envelope Sender's full address, domain, or name, or IP address. If an Envelope Sender matches entries from the `altsrchost` command, that information is printed in this section. Note that the virtual gateway address assigned at this point may be overridden by message filter processing below. For more information, see "Using Virtual Gateway™ Technology" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Bounce Profiles	Bounce profiles are applied at three different points in the processing. This is the first occurrence. If a listener has a bounce profile assigned to it, it is assigned at this point in the process. That information is printed in this section. For more information, see "Handling Undeliverable Email" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Work Queue Operations	
	The following group of functions are performed on messages in the work queue. This occurs after the message has been accepted from the client, but before the message is enqueued for delivery on a destination queue. "Messages in Work Queue" is reported by the `status` and `status detail` commands.
Masquerading	If you specified that the To:, From:, and CC: headers of messages should be masked (either from a static table entered from a listener or via an LDAP query), the change is noted here. You enable masquerading for the message headers on private listeners using the `listenerconfig -> edit -> masquerade -> config` subcommands. For more information, see "Configuring Masquerading" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
LDAP Routing	If LDAP queries have been enabled on a listener, the results of LDAP acceptance, re-routing, masquerading, and group queries are printed in this section. For more information, see "LDAP Queries" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Message Filters Processing	All messages filters that are enabled on the system are evaluated by the test message at this point. For each filter, the rule is evaluated, and if the end result is "true," each of the actions in that filter are then performed in sequence. A filter may contain other filters as an action, and the nesting of filters is unlimited. If a rule evaluates to "false" and a list of actions is associated with an `else` clause, those actions are evaluated instead. The results of the message filters, processed in order, are printed in this section. See "Using Message Filters to Enforce Email Policies," in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Mail Policy Processing

The mail policy processing section displays the Anti-Spam, Anti-Virus, Virus Outbreak Filter feature, and disclaimer stamping for all recipients you supplied. If multiple recipients match multiple policies in Email Security Manager, the following sections will be repeated for each matching policy. The string: "Message Going to" will define which recipients matched which policies.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Anti-Spam	This section notes messages that are not flagged to be processed by anti-spam scanning. If messages are to be processed by anti-spam scanning for the listener, the message is processed and the verdict returned is printed. If the Cisco IronPort appliance is configured to bounce or drop the messages based on the verdict, that information is printed and the `trace` command processing stops.
	Note: This step is skipped if anti-spam scanning is unavailable on the system. If anti-spam scanning is available but has not been enabled with a feature key, that information is also printed in this section.
	See "Anti-Spam" in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.
Anti-Virus	This section notes messages that are not flagged to be processed by anti-virus scanning. If messages are to be processed by anti-virus scanning for the listener, the message is processed and the verdict returned is printed. If the Cisco IronPort appliance is configured to "clean" infected messages, that information is noted. If configured to bounce or drop the messages based on the verdict, that information is printed and the `trace` command processing stops.
	Note: This step is skipped if anti-virus scanning is unavailable on the system. If anti-virus scanning is available but has not been enabled with a feature key, that information is also printed in this section.
	See "Anti-Virus" in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Virus Outbreak Filters Processing	This section notes messages that contain attachments are to bypass the Virus Outbreak Filters feature. If messages are to be processed by the Virus Outbreak Filters feature for the recipient, the message is processed and the evaluation. If the appliance is configured to quarantine, bounce, or drop the messages based on the verdict, that information is printed and the processing stops. See "Virus Outbreak Filters" in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.
Footer Stamping	This section notes whether a disclaimer text resource was appended to the message. The name of the text resource is displayed. See "Message Disclaimer Stamping" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Table 7-2   Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Delivery Operations	
The following sections note operations that occur when a message is delivered. The `trace` command prints "`Message Enqueued for Delivery`" before this section.	
Global Unsubscribe per Domain and per User	If any recipients you specified as input for the `trace` command match recipients, recipient domains, or IP addresses listed in the in the Global Unsubscribe feature, any unsubscribed recipient addresses are printed in this section. See "Using Global Unsubscribe" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Final Result	
When all processing has been printed, you are prompted with the final result. In the CLI, Answer **y** to: "Would you like to see the resulting message?"	

GUI example of the Trace Page

Figure 7-1   *Input for the Trace Page*

Figure 7-2   *Output for the Trace Page (1 of 2)*

Trace

Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		

Figure 7-3   Output for the Trace Page (2 of 2)

Domain Masquerading	
	No changes
Filter Processing	
skipper	Skipped (Inactive)
always_deliver	Rule: rcpt-to == "@mail.qa": False Rule: rcpt-to == "ironport.com": True Rule: OR: True Action: deliver()
Mail Policy Processing: Inbound (matched on policy Public Upgrade)	
Message going to:	admin@ironport.com
Anti-Spam Processing	
Evaluation:	Not Spam
Anti-Virus Processing	
Evaluation:	No Viruses Detected Elapsed Time: 0.000 sec
Actions Taken:	Delivered
VOF Processing	
Evaluation:	No threat detected
Footer Stamping	
Appended Text Resource:	footer
DomainKey Signing	
Result of DomainKeys processing:	DomainKeys signing not enabled in this listener's HAT
Message Delivery (matched on policy Public Upgrade)	
Final Envelope Sender:	pretend.sender@example.domain
Final Recipients:	admin@ironport.com

Final Message:	Received: from remotehost.example.com (HELO TEST) ([1.2.3.4])
	    by mail3.example.com with TEST; 21 Jul 2005 14:40:05 -0700
	Message-Id: <48q06k$@Public>
	X-Brightmail-Tracker: AAAAAA==
	X-BrightmailFiltered: true
	X-IronPort-Anti-Spam-Filtered: true
	X-IronPort-AV: i="3.95,134,1120460400";
	    d="scan'"; a="0:sNHT0"
	
	Subject: hello
	Content-Transfer-Encoding: base64
	Content-Type: text/plain; charset="utf-8"
	
	VGhpcyBpcyBhIHR1c3QgbWVzc2FnZS4KPT09PT09PT09PT09CuOD1eODg+OCv+ODvOOBp+OBmeOA
	guOCj+OBhOOCj+OBhOOAggpUaG1zIG1zIGEgSmFFwYW51c2UgZm9vdGVyCj09PT09PT09PQo=

Done

Gathering XML status from the GUI

- View status through XML pages, or access XML status information

programatically.

The XML Status feature provides a programmatic method to access email monitoring statistics. Note that some newer browsers can also render XML data directly.

Information from the pages in the GUI in this table is also available as dynamic XML output by accessing the corresponding URL:

GUI Page Name	Corresponding XML status URL
Mail Status	`http://`*hostname*`/xml/status`
Host Mail Status for a Specified Host	`http://`*hostname*`/xml/hoststatus?hostname=`*host*
DNS Status	`http://`*hostname*`/xml/dnsstatus`
Top Incoming Domains	`http://`*hostname*`/xml/topin`
Top Outgoing Domains[a]	`http://`*hostname*`/xml/tophosts`

[a] The default sort order for this page is by number of active recipients. You can change the order by appending "?sort=**order**" to the URL, where **order** is `conn_out`, `deliv_recip`, `soft_bounced`, or `hard_bounced`.

Common Administrative Tasks

The Framemaker Template contains the following contents:

Management of the Cisco IronPort Appliance

The following tasks allow you to easily manage the common functions within the Cisco IronPort appliance. The following operations and commands are described:

- `shutdown`
- `reboot`
- `suspend`
- `offline`
- `resume`
- `resetconfig`
- `version`
- `updateconfig`
- `upgrade`

Shutting Down the Cisco IronPort Appliance

To shut down your IronPort appliance, use the Shutdown/Suspend page available on the System Administration menu in the GUI or use the `shutdown` command in the CLI. Figure 8-1 shows how to shut down the appliance using the Shutdown/Suspend page.

Shutting down your appliance exits IronPort AsyncOS, which allows you to safely power down the appliance. You may restart the appliance at a later time without losing any messages in the delivery queue. You must enter a delay for the appliance to shutdown. The default delay is thirty (30) seconds. IronPort AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections.

Figure 8-1   Shutting Down Appliance via the GUI

Rebooting the Cisco IronPort Appliance

To reboot your IronPort appliance, use the Shutdown/Suspend page available on the System Administration menu in the GUI, or use the `reboot` command in the CLI. Figure 8-2 shows how to reboot the appliance using the Shutdown / Suspend page.

Rebooting your appliance restarts IronPort AsyncOS, which allows you to safely power down and reboot the appliance. You must enter a delay for the appliance to shutdown. The default delay is thirty (30) seconds. IronPort AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections. You may restart the appliance without losing any messages in the delivery queue.

Figure 8-2   Rebooting the Appliance via the GUI
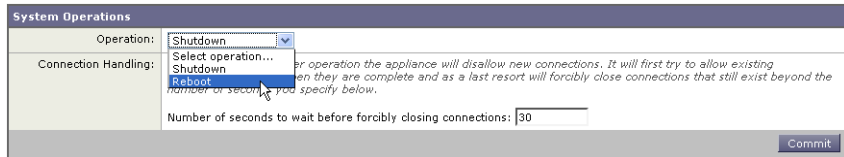
Placing the IronPort Appliance into a Maintenance State

If you want to perform system maintenance, the Cisco IronPort appliance should be placed into the offline state. The suspend and offline commands put the IronPort AsyncOS operating into offline state. The offline state is characterized by the following:

- Inbound email connections are not accepted.
- Outbound email delivery is halted.
- Log transfers are halted.
- The CLI remains accessible.

You must enter a delay for the appliance to enter the offline state. The default delay is thirty (30) seconds. IronPort AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections. If there are no open connections, the offline state commences immediately.

Note   The difference between the suspend command and the offline command is that the suspend command retains its state even after the machine is rebooted. If you issue the suspend command and reboot the appliance, you must use the resume command to return the system to an online state.

You can use the use the System Administration > Shutdown/Suspend page in the GUI to suspend email receiving and delivery on the appliance. If the appliance has multiple listeners, you can suspend and resume email receiving on individual listeners. Click **Commit** to suspend email receiving and delivery.

Figure 8-3 shows an Email Security appliance with suspended email receiving and delivery.

Figure 8-3   Suspended Mail Operations on an Appliance

The suspend and offline Commands

```
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> offline



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.
```

Resuming from an Offline State

The `resume` command in the AsyncOS CLI returns the IronPort AsyncOS operating system to normal operating state after using the `suspenddel` or `suspend` command.

You can also use the System Administration > Shutdown/Suspend page in the GUI to resume email receiving and delivery on the appliance. If the appliance has multiple listeners, you can choose to resume email receiving on individual listeners. Click **Commit** to resume email receiving and delivery.

The resume Command

```
mail3.example.com> resume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

Resetting to Factory Defaults

When physically transferring the appliance, you may want to start with factory defaults. The Reset Configuration section of the System Administration > Configuration File page, or 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 System Setup wizard or the systemsetup command after resetting the configuration.

Note   The resetconfig command only works when the appliance is in the offline state. When the resetconfig command completes, the appliance returns 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.**

The resetconfig Command

```
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.
```

Displaying the Version Information for AsyncOS

To determine which version of AsyncOS is currently installed on your Cisco IronPort appliance, use the System Overview page from the Monitor menu in the GUI (see), or use the version command in the CLI.

Support Commands

The following commands and features are useful when you are upgrading the appliance or contacting your support provider:

- Technical Support (Support Request and Remote Access pages)
- Feature Keys

Technical Support

The Technical Support section of the System Administration menu contains two pages: Support Request and Remote Access.

Remote Access

Use the Remote Access page to allow IronPort customer support remote access to your IronPort appliance.

Figure 8-4   The Remote Access Page

Edit Customer Support Remote Access

Customer Support Remote Access	
☑ Allow remote access to this appliance	
Customer Support Password:	*Cannot be the same as your admin password*
Secure Tunnel (recommended):	☑ Initiate connection via secure tunnel Port: 25
Appliance Serial Number:	XXXXXXXXXXXX-XXXXXXX

Cancel   Submit

By enabling Remote Access you are activating a special account used by IronPort Customer Support for debugging and general access to the system. This is used by IronPort Customer Support for tasks such as assisting customers in configuring their systems, understanding configurations, and investigating problem reports. You can also use the techsupport command in the CLI.

When enabling the use of the "Secure Tunnel," the appliance creates an SSH tunnel over the specified port to the server upgrades.ironport.com. By default this connection is over port 25, which will work in most environments because the

system also requires general access over that port in order to send email messages. After a connection is made to `upgrades.ironport.com`, IronPort Customer Support can to use the SSH tunnel to obtain access to the appliance. As long as the connection over port 25 is allowed, this will bypass most firewall restrictions. You can also use the `techsupport tunnel` command in the CLI.

In both the "Remote Access" and "Tunnel" modes, a password is required. It is important to understand that this is *not* the password that will be used to access the system. After the password and the system serial number are provided to your Customer Support representative, a password used to access the appliance is generated.

After the techsupport tunnel is enabled, it will remain connected to `upgrades.ironport.com` for 7 days. At the end of the 7 days, established connections will not be disconnected but will be unable to re-attach to the tunnel once disconnected. The time-out set on the SSH tunnel connection does not apply to the Remote Access account; it will remain active until specifically deactivated.

Support Request

You can use the Help > Support Request page or the `supportrequest` command (see the *Cisco IronPort AsyncOS CLI Reference Guide* for more information about the `supportrequest` command) to email the configuration of your appliance to the IronPort Customer Support team and/or additional users, and enter comments describing the issue for which you need support. This command requires that the appliance is able to send mail to the Internet.

Figure 8-5   The Support Request Page

Step 1   Enter your contact information (name, email address, phone, etc.)

Step 2   Enter a description of the issue.

Step 3   By default, the support request (including the configuration file) is sent to IronPort Customer Support (via the checkbox at the top of the form). You can also mail the configuration file to other email addresses (separate multiple addresses with commas).

Step 4   If you have a customer support ticket already for this issue, enter it.

Step 5   Click **Send**.

Step 6   A trouble ticket is created. For additional information, see IronPort Customer Support, page 1-7.

Packet Capture

Sometimes when you contact IronPort Customer Support with an issue, you may be asked to provide insight into the network activity going into and out of the Email Security appliance. The appliance provides the ability to intercept and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.

You might want to run a packet capture to debug the network setup and to discover what network traffic is reaching the appliance or leaving the appliance.

The appliance saves the captured packet activity to a file and stores the file locally. You can configure the maximum packet capture file size, how long to run the packet capture, and on which network interface to run the capture. You can also use a filter to limit the packet capture to traffic through a specific port or traffic from a specific client or server IP address.

The Support and Help > Packet Capture page in the GUI displays the list of complete packet capture files stored on the hard drive. When a packet capture is running, the Packet Capture page shows the status of the capture in progress by showing the current statistics, such as file size and time elapsed.

You can download a packet capture file using the **Download File** button and forward it in an email to IronPort Customer Support for debugging and troubleshooting purposes. You can also delete a packet capture file by selecting one or more files and clicking **Delete Selected Files**.

In the CLI, use the `packetcapture` command.

Figure 8-6 shows the Packet Capture page in the GUI.

Figure 8-6   Packet Capture Page

Packet Capture

Note   The packet capture feature is similar to the Unix tcpdump command.

Starting a Packet Capture

To start a packet capture in the CLI, run the `packetcapture > start` command. If you need to stop a running packet capture, run the `packetcapture > stop` command. The appliance stops the packet capture when the session ends.

To start a packet capture in the GUI, select the Packet Capture option under the Support and Help menu, and then click **Start Capture**. To stop a running capture, click **Stop Capture**. A running capture started in the GUI is preserved between sessions.

Note   The GUI only displays packet captures started in the GUI, not from the CLI. Similarly, the CLI only displays the status of a current packet capture run started in the CLI. Only one capture may be running at a time.

Editing Packet Capture Settings

To edit the packet capture settings in the CLI, run the `packetcapture > setup` command.

To edit packet capture settings in the GUI, select the Packet Capture option under the Support and Help menu, and then click **Edit Settings**.

Table 8-1 describes the packet capture settings you can configure.

Table 8-1   Packet Capture Configuration Options

Option	Description
Capture file size limit	The maximum file size for all packet capture files in megabytes.
Capture Duration	Choose how long to run the packet capture: • **Run Capture Until File Size Limit Reached**. The packet capture runs until the file size limit is reached. • **Run Capture Until Time Elapsed Reaches**. The packet capture runs until the configured time has passed. You can enter the time in seconds (s), minutes (m), or hours (h). If you enter the amount of time without specifying the units, AsyncOS uses seconds by default. This option is only available in the GUI. **Note** The packet capture file is split into ten parts. If the file reaches the maximum size limit before the entire time has elapsed, the oldest part of the file is deleted (the data is discarded) and a new part starts with the current packet capture data. Only 1/10 of the packet capture file is discarded at a time. • **Run Capture Indefinitely**. The packet capture runs until you manually stop it. **Note** If the file reaches the maximum size limit before you manually stop the packet capture, the oldest part of the file is deleted (the data is discarded) and a new part starts with the current packet capture data. You can always manually stop any packet capture.

Table 8-1   Packet Capture Configuration Options

Option	Description
Interface	Select the network interface on which to run the packet capture.
Filters	Choose whether or not to apply a filter to the packet capture to reduce the amount of data stored in the packet capture.
	You can use of the predefined filters to filter by port, client IP, or server IP (GUI only), or you can create a custom filter using any syntax supported by the Unix tcpdump command, such as `host 10.10.10.10 && port 80`.

AsyncOS uses the new packet capture settings after you submit them. You do not need to commit the changes.

Figure 8-7 shows where you can edit the packet capture settings in the GUI.

Figure 8-7   Edit Packet Capture Settings Page

Edit Packet Capture Settings

Note: Packet capture settings will be available for use immediately when submitted.

Working with Feature Keys

Occasionally, your support team may provide a key to enable specific functionality on your system. Use the System Administration > Feature Keys page in the GUI (or the `featurekey` command in the CLI) to enter the key and enable the associated functionality.

Keys are specific to the serial number of your appliance and specific to the feature being enabled (you cannot re-use a key from one system on another system). If you incorrectly enter a key, an error message is generated.

Feature keys functionality is split into two pages: Feature Keys and Feature Key Settings.

The Feature Keys Page

Log in to the GUI and click the System Administration tab. (For information about how to access the GUI, see the "Overview" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.) Click the Feature Keys link in the left menu. The Feature Keys page:

- Lists all active feature keys for the appliance

- Shows any feature keys that are pending activation

- Looks for new keys that have been issued (optional, and also can install keys)

A list of the currently enabled features is displayed. The Pending Activation section is a list of feature keys that have been issued for the appliance but have not yet been activated. Your appliance may check periodically for new keys depending on your configuration. You can click the **Check for New Keys** button to refresh the list of pending keys.

Feature Key Settings

The Feature Key Settings page is used to control whether your appliance checks for and downloads new feature keys, and whether or not those keys are automatically activated.

Figure 8-8   The Feature Key Settings Page

Figure 8-9   The Feature Keys Page

To add a new feature key manually, paste or type the key into the Feature Key field and click **Submit Key**. An error message is displayed if the feature is not added (if the key is incorrect, etc.), otherwise the feature key is added to the display.

To activate a new feature key from the Pending Activation list, select the key (mark the "Select" checkbox) and click **Activate Selected Keys**.

You can configure your IronPort appliance to automatically download and install new keys as they are issued. In this case, the Pending Activation list will always be empty. You can tell AsyncOS to look for new keys at any time by clicking the **Check for New Keys** button, even if you have disabled the automatic checking via the Feature Key Settings page.

Expired Feature Keys

If the feature key for the feature you are trying to access (via the GUI) has expired, please contact your IronPort representative or support organization.

Adding Users

The IronPort appliance provides two methods for adding user accounts: creating user accounts on the IronPort appliances itself, and enabling user authentication using your own centralized authentication system, which can be either an LDAP or RADIUS directory. You can manage users and connections to external authentication sources on the System Administration > Users page in the GUI (or by using the `userconfig` command in the CLI). For information about using an external directory to authenticate users, see External Authentication, page 8-330.

The default user account for the system, admin, has all administrative privileges. The admin user account cannot be edited or deleted, aside from changing the password. To change the password for the default admin user account, use the Edit User page in the GUI (see Editing Users, page 8-328 for more information) or use the `password` or `passwd` command in the CLI.) If you forget the password for the admin user account, contact your customer support provider to reset the password.

For each new user account you create on the IronPort appliance, you specify a username and a full name, and then assign the user to one of the following user roles: Administrator, Operator, Guest, Read-Only Operator, or Help Desk User. Each role contains differing levels of permissions within the system. After you have assigned a role, you specify a password for the user.

Table 8-2   *User Types Listing*

User Role	Description
Administrator	User accounts with the Administrator role have full access to all configuration settings of the system. However, only the admin user can issue the `resetconfig` and `upgrade` commands. **Note** AsyncOS does not support multiple administrators configuring the Email Security appliance from the GUI simultaneously.
Operator	User accounts with the Operator role are restricted from: • Creating or editing user accounts • Issuing the `resetconfig` command • Issuing the `systemsetup` command or running the System Setup Wizard • Issuing the `adminaccessconfig` command • Performing some quarantine functions (including creating and deleting quarantines) Otherwise, they have the same privileges as the Administrator role.
Guest	Users accounts with the Guest role can only view status information. Users with the Guest role can also manage messages in the IronPort Spam Quarantine and system quarantines, if access is enabled. Users with the Guest role cannot access Message Tracking.

Table 8-2   User Types Listing

User Role	Description
Read-Only Operator	User accounts with the Read-Only Operator role have access to view configuration information. Users with the Read-Only Operator role can make and submit changes to see how to configure a feature, but they cannot commit them. Users with this role can manage messages in the IronPort Spam Quarantine and system quarantines, if access is enabled. Users with this role cannot access the file system, FTP, or SCP.
Help Desk User	User accounts with the Help Desk User role are restricted to: • Message Tracking • Managing the IronPort Spam Quarantine and system quarantines Users with this role cannot access to the rest of the system, including the CLI. You need to enable access to the IronPort Spam Quarantine and system quarantines before a user with this role can manage them.

Note that these roles can access both the GUI and the CLI, except the Help Desk User role, which cannot access the CLI.

Although there is no limit to the number of user accounts that you can create on the appliance, you cannot create user accounts with names that are reserved by the system. For example, you cannot create the user accounts named "operator" or "root."

If you use an LDAP directory to authenticate users, you assign directory groups to user roles instead of individual users. When you assign a directory group to a user role, each user in that group receives the permissions defined for the user role. For more information, see External Authentication, page 8-330.

Managing Users

Log in to the GUI and select Users in the System Administration menu.

Figure 8-10   The Users Page

Users

The Users page lists the existing users for the system, including the username, full name, and user type or group.

From the Users page, you can:

* Add new users
* Delete users
* Edit users (including changing the admin user's password)

You can also enable the appliance to use an LDAP or RADIUS directory to authenticate users. For more information, see External Authentication, page 8-330.

Adding Users

To add a user:

Step 1   Click **Add User.** The Add User page is displayed:

Figure 8-11   Adding a User

Add Local User

Step 2   Enter a name for the user. Some words are reserved (such as "operator" or "root").

Step 3   Enter a full name for the user.

Step 4   Select a user type. (See Table 8-2 for more information about user types.)

Step 5   Enter a password and retype it. Passwords must be at least 6 characters long.

Step 6   Submit and commit your changes.

Editing Users

To edit a user (change a password, etc.):

Step 1   Click the user's name in the Users listing. The Edit User page is displayed.

Step 2   Make changes to the user.

Step 3   Submit and commit your changes.

Deleting Users

To delete a user:

Step 1   Click the trash can icon corresponding to the user's name in the Users listing.

Step 2   Confirm the deletion by clicking **Delete** in the warning dialog that appears.

Step 3   Commit your changes.

Changing Your Password

Users can change their own passwords via the Options > Change Password link at the top of the GUI.

Enter the old password then enter the new password and retype it for confirmation. Click **Submit**. You are logged out and taken to the log in screen.

Additional Commands to Support Multiple Users: who, whoami, and last

The following commands support multiple user access to the appliance.

- 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:

```
mail3.example.com> who


Username  Login Time  Idle Time  Remote Host  What

========  ==========  =========  ===========  ====

admin     03:27PM     0s         10.1.3.201   cli
```

- The `whoami` command displays the username and full name of the user currently logged in, and which groups the user belongs to:

```
mail3.example.com> whoami


Username: admin

Full Name: Administrator

Groups: admin, operators, config, log, guest
```

- The `last` command displays which users have recently logged into the appliance. The IP address of the remote host, and the login, logout, and total time are also displayed.

```
mail3.example.com> last


Username  Remote Host  Login Time        Logout Time       Total Time

========  ===========  ================  ================  ==========

Username  Remote Host  Login Time        Logout Time       Total Time
```

```
========  ===========  ================  ================  ==========

admin     10.1.3.67    Sat May 15 23:42  still logged in   15m

admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m

admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m

admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m

shutdown                                 Fri May 14 16:22

shutdown                                 Fri May 14 16:15

admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m

admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m

admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m

admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m

admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

External Authentication

If you store user information in an LDAP or RADIUS directory on your network, you can configure your IronPort appliance to use the external directory to authenticate users who log in to the appliance. To set up the appliance to use an external directory for authentication, use the System Administration > Users page in the GUI or the `userconfig` command and the `external` subcommand in the CLI.

When external authentication is enabled and a user logs into the Email Security appliance, the appliance first determines if the user is the system defined "admin" account. If not, then the appliance checks the first configured external server to determine if the user is defined there. If the appliance cannot connect to the first external server, the appliance checks the next external server in the list.

For LDAP servers, if the user fails authentication on any external server, the appliance tries to authenticate the user as a local user defined on the Email Security appliance. If the user does not exist on any external server or on the appliance, or if the user enters the wrong password, access to the appliance is denied.

If an external RADIUS server cannot be contacted, the next server in the list is tried. If all servers cannot be contacted, the appliance tries to authenticate the user as a local user defined on the Email Security appliance. However, if an external RADIUS server rejects a user for any reason, such as an incorrect password or the user being absent, access to the appliance is denied.

Figure 8-12   Enabling External Authentication

Enabling LDAP Authentication

In addition to using an LDAP directory to authenticate users, you can assign LDAP groups to IronPort user roles. For example, you can assign users in the IT group to the Administrator user role, and you can assign users in the Support group to the Help Desk User role. If a user belongs to multiple LDAP groups with different user roles, AsyncOS grants the user the permissions for the most restrictive role. For example, if a user belongs to a group with Operator permissions and a group with Help Desk User permissions, AsyncOS grants the user the permissions for the Help Desk User role.

Note   If an external user changes the user role for their LDAP group, the user should log out of the appliance and then log back in. The user will have the permissions of their new role.

Before enabling external authentication using LDAP, define an LDAP server profile and an external authentication query for the LDAP server. For more information, see the "LDAP Queries" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

To enable external authentication using LDAP:

Step 1   On the System Administration > Users page, click **Enable**. The Edit External Authentication page is displayed.

Step 2   Select the Enable External Authentication check box.

Step 3   Select LDAP for the authentication type.

Figure 8-13   Enabling External Authentication Using LDAP

Edit External Authentication

External Authentication Settings	
☑ **Enable External Authentication**	
Authentication Type:	LDAP ⌄
External Authentication Cache Timeout: ⓘ	0 seconds
LDAP External Authentication Query:	LDAP.externalauth ⌄
Timeout To Wait For Valid Response From Server:	10 seconds
Group Mapping:	Group Name in Directory — Role ⓘ — Add Row

Group names are case-sensitive.

Cancel   Submit

Step 4   Enter the amount of time to store external authentication credentials in the web user interface.

Step 5   Select the LDAP external authentication query that authenticates users.

Step 6   Enter the number of seconds that the appliance waits for a response from the server before timing out.

Step 7   Enter the name of a group from the LDAP directory that you want the appliance to authenticate, and select the role for the users in the group.

Step 8   Optionally, click **Add Row** to add another directory group. Repeat steps 7 and 8 for each directory group that the appliance authenticates.

Step 9   Submit and commit your changes.

Enabling RADIUS Authentication

You can also use a RADIUS directory to authenticate users and assign groups of users to IronPort roles. The RADIUS server should support the CLASS attribute, which AsyncOS uses to assign users in the RADIUS directory to IronPort user roles. AsyncOS supports two authentication protocols for communicating with the RADIUS server: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

To assign RADIUS users to IronPort User roles, first set the CLASS attribute on the RADIUS server with a string value of <radius-group>, which will be mapped to IronPort user roles. The CLASS attribute may contain letters, numbers, and a dash, but cannot start with a dash. AsyncOS does not support multiple values in the CLASS attribute. RADIUS users belonging to a group without a CLASS attribute or an unmapped CLASS attribute cannot log into the appliance.

If the appliance cannot communicate with the RADIUS server, the user can log in with a local user account on the appliance.

Note If an external user changes the user role for their RADIUS group, the user should log out of the appliance and then log back in. The user will have the permissions of their new role.

To enable external authentication using RADIUS:

Step 1 On the System Administration > Users page, click **Enable**. The Edit External Authentication page is displayed.

Step 2 Select the Enable External Authentication check box.

Step 3 Select RADIUS for the authentication type.

Figure 8-14   Enabling External Authentication Using RADIUS

Step 4 Enter the host name for the RADIUS server.

Step 5 Enter the port number for the RADIUS server. The default port number is 1812.

Step 6   Enter the Shared Secret password for the RADIUS server.

> ✎
>
> **Note**   When enabling external authentication for a cluster of IronPort appliances, enter the same Shared Secret password on all appliances in the cluster.

Step 7   Enter the number of seconds that the appliance waits for a response from the server before timing out.

Step 8   Select whether to use PAP or CHAP for RADIUS authentication.

Step 9   Optionally, click **Add Row** to add another RADIUS server. Repeat steps 6 and 7 for each RADIUS server that your appliance uses for authentication.

Step 10   Enter the amount of time to store external authentication credentials in the web user interface.

Step 11   Select whether to map a group of RADIUS users to an IronPort role, or grant all RADIUS users the Administrator role. It is recommended that you map RADIUS groups to IronPort roles.

Step 12   If you chose to map a RADIUS group to an IronPort role, enter the RADIUS CLASS attribute for the group and select the role for users with that CLASS attribute.

Step 13   Optionally, click **Add Row** to add another group. Repeat steps 12 and 13 for each group of users that the appliance authenticates.

Step 14   Submit and commit your changes.

Managing the Configuration File

All configuration settings within the Cisco IronPort appliance can be managed via a single configuration file. The file is maintained in XML (Extensible Markup Language) format.

You can use this file in several ways:

- You can save the configuration file to a different system to back up and preserve crucial configuration data. If you make a mistake while configuring your appliance, you can "roll back" to the most recently saved configuration file.

- You can download the existing configuration file to view the entire configuration for an appliance quickly. (Many newer browsers include the ability to render XML files directly.) This may help you troubleshoot minor errors (like typographic errors) that may exist in the current configuration.

- You can download an existing configuration file, make changes to it, and upload it to the same appliance. This, in effect, "bypasses" both the CLI and the GUI for making configuration changes.

- You can upload entire configuration file via FTP access, or you can paste portions of or an entire configuration file directly into the CLI.

- Because the file is in XML format, an associated DTD (document type definition) that describes all of the XML entities in the configuration file is also provided. You can download the DTD to validate an XML configuration file before uploading it. (XML Validation tools are readily available on the Internet.)

Managing Multiple Appliances with XML Configuration Files

- You can download an existing configuration file from one Cisco IronPort appliance, make changes to it, and upload it to a different appliance. This lets you manage an installation of multiple IronPort appliances more easily. Currently you may not load configuration files from C/X-Series appliances onto an M-Series appliance.

- You can divide an existing configuration file downloaded from one Cisco IronPort into multiple subsections. You can modify those sections that are common among all appliances (in a multiple appliance environment) and load them onto other appliances as the subsections are updated.

  For example, you could use an appliance in a test environment for testing the Global Unsubscribe command. When you feel that you have configured the Global Unsubscribe list appropriately, you could then load the Global Unsubscribe configuration section from the test appliance to all of your production appliances.

Managing Configuration Files via the GUI

To use the GUI to manage configuration files on your IronPort appliance, click the Configuration File link on the System Administration tab.

The Configuration File page contains three sections:

- **Current Configuration** - used to save and export the current configuration file.
- **Load Configuration** - used to load a complete or partial configuration file.
- **Reset Configuration** - used to reset the current configuration back to the factory defaults (you should save your configuration prior to resetting it).

Saving and Exporting the Current Configuration File

Using the Current Configuration section of the System Administration > Configuration File page, you can save the current configuration file to your local machine, save it on the appliance (placed in the `configuration` directory in the FTP/SCP root), or email it to the address specified.

Figure 8-15   Current Configuration File

You can mask the user's passwords by clicking the checkbox. Masking a password causes the original, encrypted password to be replaced with "*****" in the exported or saved file. Please note, however, that configuration files with masked passwords cannot be loaded back into AsyncOS.

Loading a Configuration File

Use the Load Configuration section of the System Administration > Configuration File page to load new configuration information into the Cisco IronPort appliance. You can load information in one of three methods:

- Placing information in the `configuration` directory and uploading it.
- Uploading the configuration file directly from your local machine.
- Pasting configuration information directly into the GUI.

Configuration files with masked passwords cannot be loaded.

Figure 8-16   Loading a Configuration File
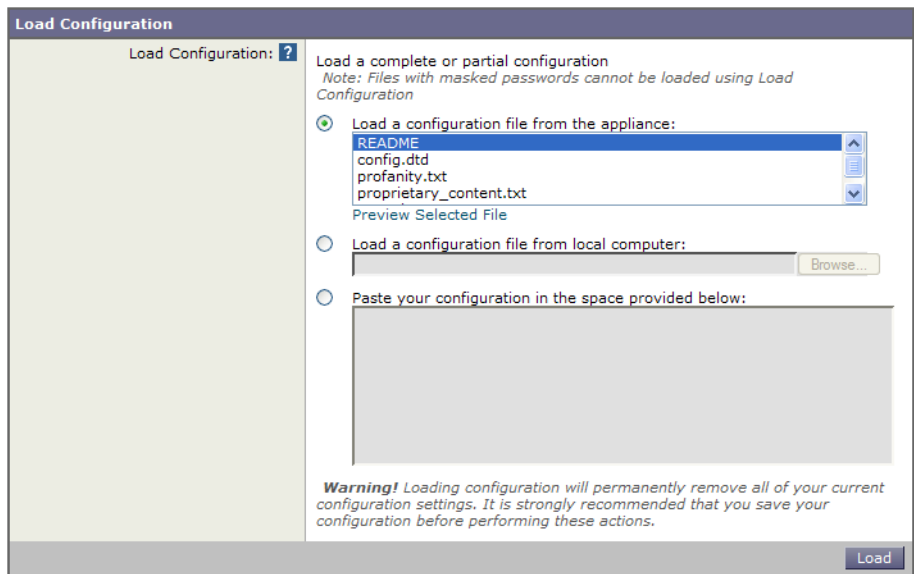
Regardless of the method, you must include the following tags at the top of your configuration:

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>
```

```
 ... your configuration information in valid XML

</config>
```

The closing `</config>` tag should follow your configuration information. The values in XML syntax are parsed and validated against the DTD (document type definition) located in the `configuration` directory on your IronPort appliance. The DTD file is named `config.dtd`. If validation errors are reported at the command line when you use the `loadconfig` command, the changes are not loaded. You can download the DTD to validate configuration files outside of the appliance before uploading them.

In either method, you can import an entire configuration file (the information defined between the highest level tags: `<config></config>`), or a *complete* and *unique* sub-section of the configuration file, as long as it contains the declaration tags (above) and is contained within the `<config></config>` tags.

"Complete" means that the entire start and end tags for a given subsection as defined by the DTD are included. For example, uploading or pasting this:

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosu

</config>
```

will cause validation errors, while uploading. This, however:

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>
```

```
    <autosupport_enabled>0</autosupport_enabled>
```

```
</config>
```

will not.

"Unique" means that the subsection of the configuration file being uploaded or pasted is not ambiguous for the configuration. For example, a system can have only one hostname, so uploading this (including the declarations and <config></config> tags):

```
<hostname>mail4.example.com</hostname>
```

is allowed. However, a system can have multiple listeners defined, each with different Recipient Access Tables defined, so uploading only this:

```
    <rat>

      <rat_entry>

        <rat_address>ALL</rat_address>

        <access>RELAY</access>

      </rat_entry>

    </rat>
```

is considered ambiguous and is not allowed, even though it is "complete" syntax.

⚠

Warning   **When uploading or pasting a configuration file or subsections of a configuration file, you have the potential to erase uncommitted changes that may be pending.**

Empty vs. Omitted Tags

Use caution when uploading or pasting sections of configuration files. If you do not include a tag, then its value in the configuration is not modified when you load a configuration file. However, if you include an empty tag, then its configuration setting is cleared.

For example, uploading this:

`<listeners></listeners>`

will remove all listeners from the system!

⚠

Warning   **When uploading or pasting subsections of a configuration file, you have the potential to disconnect yourself from the GUI or CLI and to destroy large amounts of configuration data. Do not disable services with this command if you are not able to reconnect to the appliance using another protocol, the Serial interface, or the default settings on the Management port. Also, do not use this command if you are unsure of the exact configuration syntax as defined by the DTD. Always back up your configuration data prior to loading a new configuration file.**

Note About Loading Passwords for Log Subscriptions

If you attempt to load a configuration file that contains a log subscription that requires a password (for example, one that will use FTP push), the `loadconfig` command does not warn you about the missing password. The FTP push will fail and alerts will be generated until you configure the correct password using the `logconfig` command.

Note About Character Set Encoding

The "encoding" attribute of the XML configuration file must be "`ISO-8859-1`" regardless of the character set you may be using to manipulate the file offline. Note that the encoding attribute is specified in the file whenever you issue the `showconfig`, `saveconfig`, or `mailconfig` commands:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

Currently, only configuration files with this encoding can be loaded.

Resetting the Current Configuration

Resetting the current configuration causes your IronPort Appliance to revert back to the original factory defaults. You should save your configuration prior to resetting it. Resetting the configuration via this button in the GUI is not supported in a clustering environment.

Figure 8-17   Resetting the Configuration File

Reset Configuration

Warning! Resetting your configuration will revert your appliance to factory default settings. It is strongly recommended that you save your configuration before performing these actions.
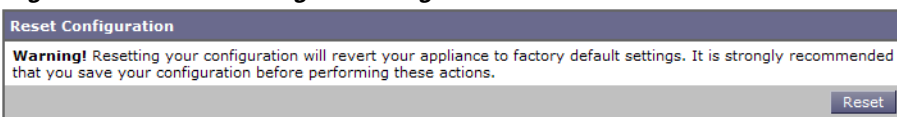
Reset

See Resetting to Factory Defaults, page 8-311.

CLI Commands for Configuration Files

The following commands allow you to manipulate the configuration files:

- showconfig

- mailconfig

- saveconfig

- loadconfig

- resetconfig (See Resetting to Factory Defaults, page 8-311.)

The showconfig, mailconfig, and saveconfig Commands

For the configuration commands showconfig, mailconfig, and saveconfig, you are prompted to choose whether to include passwords in the file that will be mailed or displayed. Choosing not to include passwords will leave any password field blank. You can choose not to include passwords if you are concerned about security breaches. However, configuration files without passwords will fail when loaded using the loadconfig command. See Note About Loading Passwords for Log Subscriptions, page 8-340.

Note When saving, showing, or mailing your configuration file if you choose to include passwords (answer yes to "Do you want to include passwords?") the passwords are encrypted. However, the private keys and certificates are included in unencrypted PEM format.

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

```
mail3.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.]
```

Use the `mailconfig` command to email the current configuration to a user. A configuration file in XML format named `config.xml` will be attached to the message.

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send

the configuration file.

[]> administrator@example.com


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


The configuration file has been sent to administrator@example.com.
```

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

```
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>
```

The loadconfig Command

Use the `loadconfig` to load new configuration information into the Cisco IronPort appliance. You can load information in one of two methods:

Step 1   Placing information in the `configuration` directory and uploading it.

Step 2   Pasting configuration information directly into the CLI.

See Loading a Configuration File, page 8-337 for more information.

Uploading Configuration Changes via the CLI

Step 1   Outside of the CLI, ensure that you are able to access the `configuration` directory of the appliance. See Appendix A, "Accessing the Appliance" for more information.

Step 2   Place an entire configuration file or subsection of a configuration file in the `configuration` directory of the appliance, or edit an existing configuration that was created from the `saveconfig` command.

Step 3   Within the CLI, use the `loadconfig` command to load the configuration file you placed in the directory from Step 2, or paste the text (XML syntax) directly into the CLI.

In this example, a file named `changed.config.xml` is uploaded and the changes are committed:

```
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
```

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. (For more information, see "Setup and Installation"
in the *Cisco IronPort AsyncOS for Email Configuration Guide*.) Finally, the
changes are committed.

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

```
1. Paste via CLI
```

```
2. Load from file
```

```
[1]> 1
```

```
Paste the configuration file now. Press CTRL-D on a blank line when
done.
```

```
[The configuration file is pasted until the end tag </config>.
Control-D is entered on a separate line.]
```

```
Values have been loaded.
```

```
Be sure to run "commit" to make these settings active.

mail3.example.com> systemsetup



[The system setup wizard is run.]



mail3.example.com> commit



Please enter some comments describing your changes:

[]> pasted new configuration file and changed default settings via

systemsetup
```

Managing Secure Shell (SSH) Keys

The sshconfig command adds and deletes secure shell (SSH) public User keys to the authorized_keys file of user accounts that have been configured on the system, including the admin account. This allows authentication to user accounts using SSH keys rather than password challenge. Both SSH protocol version 1 (SSH1) and SSH protocol version 2 (SSH2) with RSA-based authentication and DSA key types are supported. You can disable SSH1 via the setup subcommand.

✎

Note   To configure Host keys, which are used when performing SCP pushes of log files from the Cisco IronPort appliance to other host machines, use logconfig -> hostkeyconfig. For more information, see Chapter 5, "Logging."

Using hostkeyconfig, you can scan for keys of remote hosts and add them to the Cisco IronPort appliance.

Note When pasting new keys directly into the CLI, type Enter or Return on a blank line to finish entering the key.

In the following example, a new public key is installed 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)
```

```
                 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:

```
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
```

Remote SSH Command Execution

The CLI allows commands to be run via remote SSH command execution. See Appendix A, "AsyncOS Quick Reference Guide" in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide* for a list of commands. For example, the following command can be run from a remote host unchallenged if an SSH public key has been configured for the admin account on the IronPort appliance:

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003
```

Managing Secure Shell (SSH) Keys

```
System status: online

[rest of command deleted]
```

Testing and Troubleshooting

This chapter contains the following sections:

- Debugging Mail Flow Using Test Messages: Trace, page 9-352
- Using the Listener to Test the Appliance, page 9-373
- Troubleshooting the Network, page 9-378
- Troubleshooting the Listener, page 9-387
- Troubleshooting Delivery, page 9-389
- Troubleshooting Performance, page 9-392

There are some basic strategies you can employ in order to troubleshoot and solve problems with the system. However, it is important to remember that IronPort Systems offers Technical Support for complex issues (see IronPort Customer Support, page 1-7).

Note   Several of the features or commands described in this section will affect, or be affected by routing precedence. Please see Appendix B, "Assigning Network and IP Addresses" in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Debugging Mail Flow Using Test Messages: Trace

You can use System Administration > Trace page (the equivalent of the `trace` command in the CLI) to debug the flow of messages through the system by emulating sending a test message. The Trace page (and `trace` CLI command) emulates a message as being accepted by a listener and prints a summary of features that would have been "triggered" or affected by the current configuration of the system. The test message is not actually sent. The Trace page (and `trace` CLI command) can be a powerful troubleshooting or debugging tool, especially if you have combined many of the advanced features available on the Cisco IronPort appliance.

The Trace page (and `trace` CLI command) prompts you for the input parameters listed in Table 9-1.

Table 9-1   *Input for the Trace page*

Value	Description	Example
Source IP address	Type the IP address of the remote client to mimic the source of the remote domain. **Note:** The `trace` command prompts for an IP address and a fully-qualified domain name. It does *not* attempt to reverse the IP address to see if it matches the fully-qualified domain name. The `trace` command does not allow the fully-qualified domain name field to be blank, so it is impossible to test a scenario where the DNS does not reverse match properly.	`203.45.98.109`
Fully Qualified Domain Name of the Source IP	Type the fully-qualified remote domain name to mimic.	`smtp.example.com`
Listener to Trace Behavior on	Choose from the list of listeners configured on the system to emulate sending the test message to.	`InboundMail`

Table 9-1   Input for the Trace page (continued)

Value	Description	Example
SenderBase Network Owner Organization ID	Type the unique identification number of the SenderBase network owner, or allow the system to Lookup network owner ID associated with source IP address. You can view this information if you added network owners to sender groups via the GUI.	**34**
SenderBase Reputation Score (SBRS scores)	Type the SBRS you want to provide for the spoofed domain, or allow the system to lookup SBRS associated with source IP address. This can be helpful when testing policies that use SBRS scores. See "Implementing Reputation Filtering in a Listener's HAT" in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.	**-7.5**
Envelope Sender	Type the Envelope Sender of the test message.	**admin@example.net**
Envelope Recipients	Type a list of recipients for the test message. Separate multiple entries with commas.	**joe frank@example.com**
Message Body	Type the message body for the test message. Type a period on a separate line to end entering the message body. Note that "headers" are considered part of a message body.	**To: 1@example.com** From: ralph Subject: Test **this is a test message** **.**

After you have entered the values, click **Start Trace**. A summary of all features configured on the system affecting the message is printed.

You can upload message bodies from your local file system. (In the CLI, you can test with message bodies you have uploaded to the `/configuration` directory. See Appendix A, "Accessing the Appliance" for more information on placing files for import onto the Cisco IronPort appliance.)

After the summary is printed, you are prompted to view the resulting message and re-run the test message again. If you enter another test message, the Trace page and the `trace` command uses any previous values from Table 9-1 you entered.

Note The sections of configuration tested by the `trace` command listed in Table 9-2 are performed *in order*. This can be extremely helpful in understanding how the configuration of one feature affects another. For example, a recipient address transformed by the domain map feature will affect the address as it is evaluated by the RAT. A recipient that is affected by the RAT will affect the address as it is evaluated by alias table, and so on.

Table 9-2   Viewing Output When Performing a Trace

trace Command Section	Output
Host Access Table (HAT) and Mail Flow Policy Processing	The Host Access Table settings for the listener you specified are processed. The system reports which entry in the HAT matched from the remote IP address and remote domain name you entered. You can see the default mail flow policies and sender groups and which one matched the given entries.
	If the Cisco IronPort appliance was configured to reject the connection (either through a REJECT or TCPREFUSE access rule), the `trace` command exits at the point in the processing.
	For more information on setting HAT parameters, see "The Host Access Table (HAT): Sender Groups and Mail Flow Policies" in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Envelope Sender Address Processing

These sections summarize how the appliance configuration affects the Envelope Sender you supply. (That is, how the MAIL FROM command would be interpreted by the configuration of the appliance.) The `trace` command prints "`Processing MAIL FROM:`" before this section.

Default Domain	If you specified that a listener to change the default sender domain of messages it receives, any change to the Envelope Sender is printed in this section.
	For more information, see the "Customizing Listeners" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Masquerading	If you specified that the Envelope Sender of a message should be transformed, the change is noted here. You enable masquerading for the Envelope Sender on private listeners using the `listenerconfig -> edit -> masquerade -> config` subcommands. For more information, see the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Envelope Recipient Processing

These sections summarize how the appliance affects the Envelope Recipients you supply. (That is, how the RCPT TO command would be interpreted by the configuration of the appliance.) The `trace` command prints "`Processing Recipient List:`" before this section.

Default Domain	If you specified that a listener to change the default sender domain of messages it receives, any changes to the Envelope Recipients are printed in this section. For more information, see the "Customizing Listeners" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Domain Map Translation	The domain map feature transforms the recipient address to an alternate address. If you specified any domain map changes and a recipient address you specified matches, the transformation is printed in this section. For more information, see the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Recipient Access Table (RAT)	Each Envelope Recipient that matches an entry in the RAT is printed in this section, in addition to the policy and parameters. (For example, if a recipient was specified to bypass limits in the listener's RAT.) For more information on specifying recipients you accept, see the "Configuring the Gateway to Receive Email" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.
Alias Table	Each Envelope Recipient that matches an entry in the alias tables configured on the appliance (and the subsequent transformation to one or more recipient addresses) is printed in this section. For more information, see the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Pre-Queue Message Operations

These sections summarize how the appliance affects each message after the message contents have been received, but before the messages are enqueued on the work queue. This processing occurs before the final `250 ok` command is returned to the remote MTA.

The `trace` command prints "Message Processing:" before this section.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Virtual Gateways	The `altsrchost` command assigns messages to a specific interface, based on a match of the Envelope Sender's full address, domain, or name, or IP address. If an Envelope Sender matches entries from the `altsrchost` command, that information is printed in this section. Note that the virtual gateway address assigned at this point may be overridden by message filter processing below. For more information, see the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Bounce Profiles	Bounce profiles are applied at three different points in the processing. This is the first occurrence. If a listener has a bounce profile assigned to it, it is assigned at this point in the process. That information is printed in this section. For more information, see the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 9-2   *Viewing Output When Performing a Trace (continued)*

trace Command Section	Output
Work Queue Operations The following group of functions are performed on messages in the work queue. This occurs after the message has been accepted from the client, but before the message is enqueued for delivery on a destination queue. "Messages in Work Queue" is reported by the `status` and `status detail` commands.	
Masquerading	If you specified that the To:, From:, and CC: headers of messages should be masked (either from a static table entered from a listener or via an LDAP query), the change is noted here. You enable masquerading for the message headers on private listeners using the `listenerconfig -> edit -> masquerade -> config` subcommands. For more information, see the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
LDAP Routing	If LDAP queries have been enabled on a listener, the results of LDAP acceptance, re-routing, masquerading, and group queries are printed in this section. For more information, see the "LDAP Queries" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Message Filters Processing	All messages filters that are enabled on the system are evaluated by the test message at this point. For each filter, the rule is evaluated, and if the end result is "true," each of the actions in that filter are then performed in sequence. A filter may contain other filters as an action, and the nesting of filters is unlimited. If a rule evaluates to "false" and a list of actions is associated with an `else` clause, those actions are evaluated instead. The results of the message filters, processed in order, are printed in this section. See the "Using Message Filters to Enforce Email Policies" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

Mail Policy Processing

The mail policy processing section displays the Anti-Spam, Anti-Virus, Virus Outbreak Filter feature, and footer stamping for all recipients you supplied. If multiple recipients match multiple policies in Email Security Manager, the following sections will be repeated for each matching policy. The string: "Message Going to" will define which recipients matched which policies.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Anti-Spam	This section notes messages that are not flagged to be processed by anti-spam scanning. If messages are to be processed by anti-spam scanning for the listener, the message is processed and the verdict returned is printed. If the Cisco IronPort appliance is configured to bounce or drop the messages based on the verdict, that information is printed and the `trace` command processing stops.
	Note: This step is skipped if anti-spam scanning is unavailable on the system. If anti-spam scanning is available but has not been enabled with a feature key, that information is also printed in this section.
	See the "Anti-Spam" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Anti-Virus	This section notes messages that are not flagged to be processed by anti-virus scanning. If messages are to be processed by anti-virus scanning for the listener, the message is processed and the verdict returned is printed. If the Cisco IronPort appliance is configured to "clean" infected messages, that information is noted. If configured to bounce or drop the messages based on the verdict, that information is printed and the `trace` command processing stops. Note: This step is skipped if anti-virus scanning is unavailable on the system. If anti-virus scanning is available but has not been enabled with a feature key, that information is also printed in this section. See the "Anti-Virus" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.
Content Filters Processing	All content filters that are enabled on the system are evaluated by the test message at this point. For each filter, the rule is evaluated, and if the end result is "true," each of the actions in that filter are then performed in sequence. A filter may contain other filters as an action, and the nesting of filters is unlimited. The results of the content filters, processed in order, are printed in this section. See the "Email Security Manager" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
VOF Processing	This section notes messages that contain attachments are to bypass the Virus Outbreak Filters feature. If messages are to be processed by Virus Outbreak Filters for the recipient, the message is processed and the evaluation. If the appliance is configured to quarantine, bounce, or drop the messages based on the verdict, that information is printed and the processing stops. See the "Virus Outbreak Filters" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.
Footer Stamping	This section notes whether a footer text resource was appended to the message. The name of the text resource is displayed. See "Message Footer Stamping" in the "Text Resources" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Table 9-2   Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Delivery Operations The following sections note operations that occur when a message is delivered. The `trace` command prints "`Message Enqueued for Delivery`" before this section.	
Global Unsubscribe per Domain and per User	If any recipients you specified as input for the `trace` command match recipients, recipient domains, or IP addresses listed in the in the Global Unsubscribe feature, any unsubscribed recipient addresses are printed in this section. See the "Configuring Routing and Delivery Features" chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.
Final Result When all processing has been printed, you are prompted with the final result. In the CLI, Answer **y** to the question, "Would you like to see the resulting message?" to view the resulting message.	

GUI example of the Trace Page

Figure 9-1   *Input for the Trace Page*

Figure 9-2   *Output for the Trace Page (1 of 2)*

Trace

Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		

Figure 9-3   Output for the Trace Page (2 of 2)

Domain Masquerading	
	No changes
Filter Processing	
skipper	Skipped (Inactive)
always_deliver	Rule: rcpt-to == "@mail.qa": False Rule: rcpt-to == "ironport.com": True Rule: OR: True Action: deliver()
Mail Policy Processing: Inbound (matched on policy Public Upgrade)	
Message going to:	admin@ironport.com
Anti-Spam Processing	
Evaluation:	Not Spam
Anti-Virus Processing	
Evaluation:	No Viruses Detected Elapsed Time: 0.000 sec
Actions Taken:	Delivered
VOF Processing	
Evaluation:	No threat detected
Footer Stamping	
Appended Text Resource:	footer
DomainKey Signing	
Result of DomainKeys processing:	DomainKeys signing not enabled in this listener's HAT
Message Delivery (matched on policy Public Upgrade)	
Final Envelope Sender:	pretend.sender@example.domain
Final Recipients:	admin@ironport.com

Final Message:	Received: from remotehost.example.com (HELO TEST) ([1.2.3.4])
	  by mail3.example.com with TEST; 21 Jul 2005 14:40:05 -0700
	Message-Id: <48q06k$@Public>
	X-Brightmail-Tracker: AAAAAA==
	X-BrightmailFiltered: true
	X-IronPort-Anti-Spam-Filtered: true
	X-IronPort-AV: i="3.95,134,1120460400";
	  d="scan'"; a="0:sNHT0"
	
	Subject: hello
	Content-Transfer-Encoding: base64
	Content-Type: text/plain; charset="utf-8"
	
	VGhpcyBpcyBhIHRlc3QgbWVzc2FnZS4KPT09PT09PT09CuOD1eODg+OCv+ODvOOBp+OBmeOA
	guOCj+OBhOOCj+OBhOOAggpUaG1zIG1zIGEgdGVzdCBtZXNzYWdlLgo=

Done

CLI Example of the trace Command

```
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.

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)
```

Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide

```
      - 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


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]>
```

Using the Listener to Test the Appliance

"Black hole" listeners allow you to test your message generation systems, and to also get a rough measure of receiving performance. Two types of black hole listeners are *queueing* and *non-queueing*.

The queueing listener saves the message to the queue, but then immediately deletes it. The non-queueing listener accepts a message, and then immediately deletes it without saving it.

Use a queuing listener when you are interested in measuring the performance of the entire injection portion of your message generation system. Use the non-queueing listener when you want to troubleshoot the connection from your message generation system to the appliance.

For example, in Figure 9-4, you could create a black hole listener "C" to mirror the private listener labeled "B." A non-queueing version tests the performance path of the system from the groupware client to the groupware server to the appliance. A queueing version tests that same path *and* the appliance's ability to enqueue messages and prepare them for delivery via SMTP.

Figure 9-4   Black Hole Listener for an Enterprise Gateway
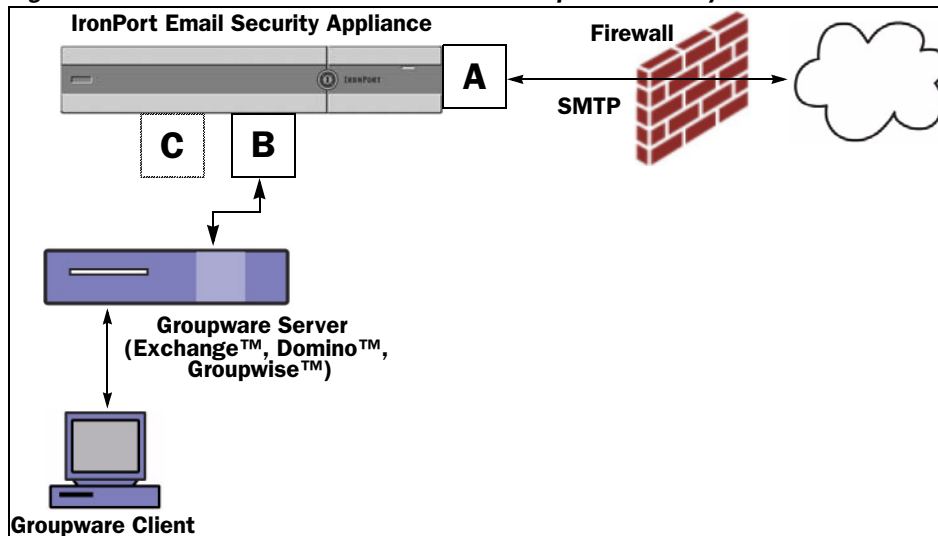
In the following example, the `listenerconfig` command is used to create a black hole queueing listener named `BlackHole_1` on the Management interface. This Host Access Table (HAT) for the listener is then edited to accept connections from the following hosts:

- `yoursystem.example.com`
- `10.1.2.29`
- `badmail.tst`
- `.tst`

Note   The final entry, `.tst`, configures the listener so that any host in the `.tst` domain can send email to the listener named `BlackHole_1`.

Example

```
mail3.example.com> listenerconfig


Currently configured listeners:
```

```
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new


Please select the type of listener you want to create.

1. Private

2. Public

3. Blackhole

[2]> 3


Do you want messages to be queued onto disk?  [N]> y


Please create a name for this listener (Ex: "OutboundMail"):

[]> BlackHole_1


Please choose an IP interface for this Listener.
```

```
1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1



Choose a protocol.

1. SMTP

2. QMQP

[1]> 1



Please enter the IP 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 addressed are allowed.

Separate multiple entries with commas.

[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst



Do you want to enable rate limiting per host? (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 BlackHole_1 created.

Defaults have been set for a Black Hole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.

```
Currently configured listeners:

1. BlackHole_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole
Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. 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.

[]>
```

(Remember to issue the `commit` command for these changes to take effect.)

After you have configured a black hole queuing listener and modified the HAT to accept connections from your injection system, use your injection system to begin sending email to the appliance. Use the `status`, `status detail`, and `rate` commands to monitor system performance. You can also monitor the system via the Graphical User Interface (GUI). For more information, see:

- Monitoring Via the CLI, page 6-234
- Other Tasks in the GUI, page 7-285

Troubleshooting the Network

If you suspect that the appliance has network connectivity issues, first confirm that the appliance is working properly.

Strategies to Test the Network Connectivity of the Appliance

To confirm that the appliance is active on the network and able to send email:

Step 1 Connect to the system and log in as the administrator. After successfully logging in, the following messages are displayed:

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.



AsyncOS x.x for Cisco IronPort



Welcome to the Cisco IronPort Messaging Gateway Appliance(tm)
```

Step 2 Use the `status` or `status detail` commands.

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

or

```
mail3.example.com> status detail
```

The `status` command returns a subset of the monitored information about email operations. The statistics returned are grouped into two categories: counters and gauges. For complete monitoring information about email operations including rates, use the `status detail` command. Counters provide a running total of various events in the system. For each counter, you can view the total number of events that have occurred since the counter was reset, since the last system reboot, and over the system's lifetime. (For more information, see Monitoring Via the CLI, page 6-234.)

Step 3 Use the `mailconfig` command to send mail to a known working address.

The `mailconfig` command generates a human-readable file including all configuration settings available to the appliance. Attempt to send the file from the appliance to a known working email address to confirm that the appliance is able to send email over the network.

```
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


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


The configuration file has been sent to user@example.com.

mail3.example.com>
```

Troubleshooting

After you have confirmed that the appliance is active on the network, use the following commands to pinpoint any network problems.

- You can use the `netstat` command to display network connections (both incoming and outgoing), routing tables, and a number of network interface statistics, including the following information:
    - List of active sockets
    - State of network interfaces
    - Contents of routing tables

- – Size of the listen queues

- – Packet traffic information

- You can use the `diagnostic -> network -> flush` command to flush all network related caches.

- You can use the `diagnostic -> network -> arpshow` command to show the system ARP cache.

- You can use the `packetcapture` command to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

  To use `packetcapture`, set the network interface and the filter. The filter uses the same format the UNIX `tcpdump` command. Use `start` to begin the packet capture and `stop` to end it. After stopping the capture, you need to use SCP or FTP to download the files from the `/pub/captures` directory. For more information, see Packet Capture, page 8-317.

- Use the `ping` command to a known working host to confirm that the appliance has an active connection on the network and is able to reach specific segments of your network.

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

```
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=9 ttl=64 time=0.133 ms

64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms

^C

--- anotherhost.example.com ping statistics ---

11 packets transmitted, 11 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

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

- Use the `traceroute` command to test connectivity to a network host from the appliance and debug routing issues with network hops.

```
mail3.example.com> traceroute



Which interface do you want to trace from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)
```

```
4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1



Please enter the host to which you want to trace the route.

[]> 10.1.1.1



Press Ctrl-C to stop.

traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets

 1  gateway (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms

 2  hostname (10.1.1.1)  0.298 ms  0.302 ms  0.291 ms

mail3.example.com>
```

- Use the `diagnostic -> network -> smtpping` command to test a remote SMTP server.
- 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.

```
mail3.example.com> nslookup



Please enter the host or IP to resolve.

[]> example.com



Choose the query type:
```

```
1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>
```

```
A=192.0.34.166 TTL=2d
```

Table 9-3   Checking DNS Functionality: 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
SOA	the domain's "start-of-authority" information
TXT	the text information

- Use the `tophosts` command via the CLI or the GUI, and sort by Active Recipients.

  The `tophosts` command returns a list of the top 20 recipient hosts in queue. This command can help you determine if network connectivity problems are isolated to a single host or group of hosts to which you are attempting to send email. (For more information, see "Determining the Make-up of the Mail Queue" on page 49.)

```
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

   ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1  aol.com36510255218

2  hotmail.com29071982813

3  yahoo.com13461231119

4  excite.com9838494
```

```
5  msn.com8427633  29
```

^C

- "Drill-down" to use the `hoststatus` command on the top domains listed from the `tophosts` command results.

  The `hoststatus` command returns monitoring information about email operations relating to a specific recipient host. DNS information stored in the AsyncOS cache and the last error returned from the recipient host are also given. Data returned is cumulative since the last `resetcounters` command. (For more information, see Monitoring the Status of a Mail Host, page 6-242.)

  Using the `hoststatus` command on the top domains can isolate the performance issues with DNS resolution to the either the appliance or the internet. For example, if the `hoststatus` command for the top active recipient host shows many pending outbound connections, then try to determine if that particular host is down or unreachable, or if the appliance cannot connect to all or the majority of hosts.

- Check firewall permissions.

  The appliance may need all of the following ports to be opened in order to function properly: ports 20, 21, 22, 23, 25, 53, 80, 123, 443, and 628. (See Appendix C, "Firewall Information," in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.)

- Send email from the appliance on your network to `dnscheck@ironport.com`

  Send an email from within your network to `dnscheck@ironport.com` to perform basic DNS checks on your system. And auto-responder email will respond with the results and details of the following four tests:

  DNS PTR Record - Does the IP address of the Envelope From match the PTR record for the domain?

  DNS A Record - Does the PTR record for the domain match the IP address of the Envelope From?

  HELO match - Does the domain listed in the SMTP HELO command match the DNS hostname in the Envelope From?

Mail server accepting delayed bounce messages - Does the domain listed in the SMTP HELO command have MX records that resolve IP addresses for that domain?

Troubleshooting the Listener

If you suspect problems with injecting email, use the following strategies:

- Confirm the IP address that you are injecting from, and then use the `listenerconfig` command to check for allowed hosts.

  Is the IP address allowed to connect to the listener you have created? Use the `listenerconfig` command to examine the Host Access Table (HAT) for the listener. Use these commands to print the HAT for a listener:

  `listenerconfig` -> `edit` -> *listener_number* -> `hostaccess` -> `print`

  The HAT can be configured to refuse connections by IP address, block of IP addresses, hostname, or domains. For more information, see "Specifying Hosts that are Allowed to Connect" on page 107.

  You can also use the `limits` subcommand to check the maximum number of connections allowed for a listener:

  `listenerconfig` -> `edit` -> *listener_number* -> `limits`

- On the machine that you are injecting from, use Telnet or FTP to manually connect to the appliance. For example:

```
injection_machine% telnet appliance_name
```

  You can also use the `telnet` command within the appliance itself to connect from the listener to the actual appliance:

```
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 '^]'.
```

If you cannot connect from one interface to another, you may have issues with the way in which the appliance's Management and Data1 and Data2 interfaces are connected to your network. Ensure that the telnet service is enabled on the target interface if you are attempting to connect using telnet. See Appendix A, "Accessing the Appliance" for more information. You can also telnet to port 25 of the listener and enter SMTP commands manually (if you are familiar with the protocol).

- Examine the IronPort text mail logs and injection debug logs to check for receiving errors.

  Injection debug logs record the SMTP conversation between the appliance and a specified host connecting to the system. Injection debug logs are useful for troubleshooting communication problems between the appliance and a

client initiating a connection from the Internet. The log records all bytes transmitted between the two systems and classifies them as "Sent to" the connecting host or "Received from" the connecting host.

For more information, see Using IronPort Text Mail Logs, page 5-167 and Using IronPort Injection Debug Logs, page 5-185.

Troubleshooting Delivery

If you suspect problems with delivering email from the appliance, try the following strategies:

- Determine if the problem is domain-specific.

  Use the `tophosts` command to get immediate information about the email queue and determine if a particular recipient domain has delivery problems.

  Are there problem domains returned when you sort by "Active Recipients?"

  When you sort by Connections Out, does any one domain reach the maximum connections specified for a listener? The default maximum number of connections for a listener is 600. The default maximum system-wide number of connections if 10,000 (set by the `deliveryconfig` command). You can examine the maximum number of connections for a listener using the command:

  `listenerconfig` -> `edit` -> *injector_number* -> `limits`

  Are the connections for a listener further limited by the `destconfig` command (either by system maximum or by Virtual Gateway addresses)? Use this command to examine the `destconfig` connection limits:

  `destconfig` -> `list`

- Use the `hoststatus` command.

  "Drill-down" using the `hoststatus` command on the top domains listed from the results listed by the `tophosts` command.

  Is the host available and accepting connections?

  Are there problems with one specific MX record mail server for the given host?

The hoststatus command reports the last "5XX" status code and description returned by the host if there is a 5XX error (Permanent Negative Completion reply) for the specified host. If the last outgoing TLS connection to the host failed, the hoststatus command displays the reason why it failed.

- Configure and/or examine the domain debug, bounce, and text mail logs to check if the recipient host is available.

   Domain debug logs record the client and server communication during an SMTP conversation between the appliance and a specified recipient host. This log file type can be used to debug issues with specific recipient hosts.

   For more information, see Using IronPort Domain Debug Logs, page 5-184.

   Bounce logs record all information pertaining to each bounced recipient.

   For more information, see Using IronPort Bounce Logs, page 5-179.

   Text mail logs contain details of email receiving, email delivery and bounces. Status information is also written to the mail log every minute. These logs are a useful source of information to understand delivery of specific messages and to analyze system performance.

   For more information, see Using IronPort Text Mail Logs, page 5-167.

- Use the telnet command to connect from the appliance to the problem domain:

```
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]> 1
```

```
Enter the remote hostname or IP.

[]> problemdomain.net



Enter the remote port.

[25]> 25
```

- You can use the `tlsverify` command to 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.

```
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.
```

Troubleshooting Performance

If you suspect that there are there are performance problems with the appliance, utilize the following strategies:

- Use the `rate` and `hostrate` commands to check the current system activity.

  The `rate` command returns real-time monitoring information about email operations. For more information, see .

  The `hostrate` command returns real-time monitoring information for a specific host.

- Use the `status` command to cross-check the historical rates to check for degradation.

- Use the `status detail` command to check the RAM utilization.

  You can use the `status detail` command to quickly see the system's RAM, CPU, and Disk I/O utilization.

Note   RAM utilization should always be less than 75%. If RAM utilization exceeds 75%, then, the appliance will enter "resource conservation mode;" it initiates a "back-off" algorithm to prevent over-subscription of resources and sends out the following email alert:

```
This system (hostname: hostname) has entered a 'resource conservation'
mode in order to prevent the rapid depletion of critical system
resources.
```

```
RAM utilization for this system has exceeded the resource conservation
threshold of 75%. The allowed injection rate for this system will be
gradually decreased as RAM utilization approaches 85%.
```

This situation occurs only with an aggressive injection with poor deliverability facilities. If you encounter RAM utilization exceeding 75%, check the number of messages in the queue and see if a particular domain is down or unavailable for delivery (via the `hoststatus` or `hostrate` commands). Also check the status of the system and ensure that delivery is not suspended. If after stopping the injection you continue to experience a high RAM utilization, contact IronPort Customer Support. See IronPort Customer Support, page 1-7.

- Is the problem specific to one domain?

   Use the `tophosts` command to get immediate information about the email queue and determine if a particular recipient domain has delivery problems.

   Check the size of the queue. You can delete, bounce, suspend, or redirect messages in the email queue to manage its size, or to deal with recipients to a specific, problematic domain. For more information, see Managing the Email Queue, page 6-258. Use these commands:

   - `deleterecipients`
   - `bouncerecipients`
   - `redirectrecipients`
   - `suspenddel` / `resumedel`
   - `suspendlistener` / `resumelistener`

Use the `tophosts` command to check the number of soft and hard bounces. Sort by "Soft Bounced Events" (option `4`) or "Hard Bounced Recipients" (option `5`). If the performance for a particular domain is problematic, use the commands above to manage the delivery to that domain.

I N D E X

S