



Cisco IronPort AsyncOS 7.6 for Email Daily Management Guide

February 6, 2012

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26344-01

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

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

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

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

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

Cisco IronPort AsyncOS 7.6 for Email Daily Management Guide
© 2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Managing the Cisco IronPort Email Appliance 1-1

- The Email Security Appliance Documentation Set 1-1
- How to Use This Guide 1-2
 - Before You Begin 1-2
 - How This Book Is Organized 1-2
 - Typographic Conventions 1-3
 - Where to Find More Information 1-3
 - Knowledge Base 1-3
 - Cisco IronPortSupport Community 1-4
 - Cisco IronPort Customer Support 1-4
 - Cisco IronPort Welcomes Your Comments 1-4

CHAPTER 2

Using Email Security Monitor 2-1

- Email Security Monitor Overview 2-1
 - Email Security Monitor and Centralized Management 2-2
- Email Security Monitor Pages 2-2
 - Searching and Email Security Monitor 2-3
 - The Overview Page 2-4
 - System Overview 2-4
 - Incoming and Outgoing Summary and Graph 2-5
 - Categorizing Email 2-6
 - How Messages are Categorized 2-7
 - Incoming Mail Page 2-7
 - Incoming Mail 2-8
 - Incoming Mail Details Listing 2-10
 - Reporting Pages Populated with Data: Sender Profile Pages 2-11
 - Sender Groups Report 2-16
 - Outgoing Destinations 2-17
 - Outgoing Senders 2-18
 - The Delivery Status Page 2-19
 - Retrying Delivery 2-20
 - Delivery Status Details Page 2-20
 - The Internal Users Page 2-21
 - Internal User Details 2-22

Searching for a Specific Internal User	2-23
The DLP Incidents Page	2-23
DLP Incidents Details	2-24
DLP Policy Detail Page	2-24
The Content Filters Page	2-25
Content Filter Details	2-25
The Outbreak Filters Page	2-26
Virus Types Page	2-28
TLS Connections Page	2-29
Rate Limits Page	2-31
The System Capacity Page	2-32
System Capacity- Workqueue	2-33
System Capacity- Incoming Mail	2-34
System Capacity-Outgoing Mail	2-35
System Capacity-System Load	2-36
Note about Memory Page Swapping	2-37
System Capacity- All	2-38
The System Status Page	2-38
System Status	2-38
Gauges	2-39
Rates	2-40
Counters	2-40
Retrieving CSV Data	2-41
Retrieving CSV Data Via Automated Processes	2-42
Reporting Overview	2-43
Scheduled Report Types	2-43
Notes on Reports	2-44
Setting the Return Address for Reports	2-44
Managing Reports	2-44
Scheduled Reports	2-45
Creating a Scheduled Report	2-45
Editing Scheduled Reports	2-46
Deleting Scheduled Reports	2-46
Archived Reports	2-46
On-Demand Reports	2-47

CHAPTER 3

Tracking Email Messages	3-1
Tracking Service Overview	3-1
Enabling and Disabling Local Message Tracking	3-2

Disabling Local Message Tracking	3-2
Understanding Tracking Query Setup	3-3
Running a Search Query	3-5
Narrowing the Result Set	3-6
Understanding Tracking Query Results	3-6
Message Details	3-7

CHAPTER 4

Quarantines 4-1

Quarantines Overview	4-1
Quarantine Types	4-1
System Quarantines	4-2
Cisco IronPort Spam Quarantines	4-2
Managing System Quarantines via the Graphical User Interface (GUI)	4-3
System Quarantine Settings	4-3
Allocating Space for System Quarantines	4-4
Retention Time	4-4
Default Action	4-4
When Allocated Space is Exceeded Send Messages and:	4-5
System Quarantine Performance	4-6
Users and User Groups	4-6
Creating System Quarantines	4-6
Editing System Quarantines	4-7
Deleting System Quarantines	4-8
Working with Messages in System Quarantines	4-8
Viewing Messages in a System Quarantine	4-9
Processing Messages in a Quarantine	4-9
Quarantined Messages and International Character Sets	4-10
Message Actions and Viewing Message Content	4-10
Viewing Matched Content	4-12
Selecting a Message Action	4-13
Sending a Copy of the Message	4-13
Testing for Viruses	4-13
Downloading Attachments	4-14
Searching System Quarantines	4-14
Multi-User Access and System Quarantines	4-15
Configuring Multi-User Access	4-15
Multi-User Access and Messages in Multiple Quarantines	4-15
System Quarantines and Virus Scanning	4-16
System Quarantines and Alerts	4-16

System Quarantines and Logging	4-16
The Outbreak Filters Feature and the Outbreak Quarantine	4-17
Manage Rule by Summary Link	4-17
Send to Cisco IronPort Systems	4-17
Configuring the Cisco IronPort Spam Quarantines Feature	4-18
Enabling and Disabling the Local Cisco IronPort Spam Quarantine	4-19
Disabling the Local Cisco IronPort Spam Quarantine	4-19
Migrating from a Local Cisco IronPort Spam Quarantine to an External Quarantine	4-20
Cisco IronPort Spam Quarantine Settings	4-21
Spam Quarantine Settings	4-21
Cisco IronPort Spam Quarantine Access	4-21
Spam Notifications	4-21
Configuring the Local Cisco IronPort Spam Quarantine	4-22
Configuring Spam Quarantine Settings for the Local Cisco IronPort Spam Quarantine	4-22
Configuring End User Quarantine Access	4-24
Configuring Spam Notifications	4-25
Configuring an External Cisco IronPort Spam Quarantine	4-27
Adding an External Cisco IronPort Spam Quarantine	4-27
Editing an External Cisco IronPort Spam Quarantine	4-27
Removing an External Cisco IronPort Spam Quarantine	4-28
Enabling the Cisco IronPort Spam Quarantine HTTP/S Service on an IP Interface	4-28
Enabling Cisco IronPort Spam Quarantines for a Mail Policy	4-29
Considerations for Deployment	4-30
Disk Space	4-31
End Users Accessing the Cisco IronPort Spam Quarantine	4-31
Example Configurations	4-32
Testing Notifications	4-32
Ensuring that End Users Receive the Notifications	4-33
Receiving Multiple Notifications	4-33
Determining Which Messages are Present for Each User	4-33
Limiting which Addresses have Mail Quarantined	4-33
Default Encoding	4-34
Managing Messages in Cisco IronPort Spam Quarantines	4-35
Searching for Messages in the Cisco IronPort Spam Quarantine	4-35
Viewing Messages in the Cisco IronPort Spam Quarantine	4-36
Delivering Messages in the Cisco IronPort Spam Quarantine	4-36
Deleting Messages from the Cisco IronPort Spam Quarantine	4-37
Working with Safelists and Blocklists	4-37
The Safelist/Blocklist Database	4-37
Creating and Maintaining Safelists and Blocklists	4-38

Message Delivery For Safelists and Blocklists	4-38
Administrator Tasks for Creating and Maintaining Safelists and Blocklists	4-39
Enabling and Configuring Safelist/Blocklist Settings	4-39
Backing Up and Restoring the Safelist/Blocklist Database	4-40
Synchronizing Safelist and Blocklist Settings and Databases	4-40
Troubleshooting Safelists and Blocklists	4-41
End User Tasks for Configuring Safelists and Blocklists	4-41
Accessing Safelists and Blocklists	4-42
Adding Entries to Safelists	4-42
Adding Entries to Blocklists	4-44

CHAPTER 5

Logging 5-1

Overview	5-1
Understanding Log Files and Log Subscriptions	5-1
Log Types	5-2
Log Type Characteristics	5-4
Log Retrieval Methods	5-6
Log Filenames and Directory Structure	5-6
Log Rollover and Transfer Schedule	5-6
Logs Enabled by Default	5-7
Log Types	5-7
Timestamps in Log Files	5-8
Using IronPort Text Mail Logs	5-8
Interpreting an IronPort Text Mail Log	5-9
Examples of Text Mail Log Entries	5-10
Log Entries for Generated or Re-Written Messages	5-14
Messages Sent to the Cisco IronPort Spam Quarantine	5-14
Using IronPort Delivery Logs	5-15
Examples of Delivery Log Entries	5-16
Using IronPort Bounce Logs	5-17
Examples of Bounce Log Entries	5-19
Using IronPort Status Logs	5-19
Reading Status Logs	5-20
Using IronPort Domain Debug Logs	5-22
Using IronPort Injection Debug Logs	5-23
Using IronPort System Logs	5-24
Using IronPort CLI Audit Logs	5-25
Using IronPort FTP Server Logs	5-26
Using IronPort HTTP Logs	5-27

Using IronPort NTP Logs	5-28
Using Scanning Logs	5-28
Using IronPort Anti-Spam Logs	5-29
Using IronPort Anti-Virus Logs	5-29
Using IronPort Spam Quarantine Logs	5-30
Using IronPort Spam Quarantine GUI Logs	5-30
Using IronPort LDAP Debug Logs	5-31
Using Safelist/Blocklist Logs	5-32
Using Reporting Logs	5-33
Using Reporting Query Logs	5-34
Using Updater Logs	5-35
Understanding Tracking Logs	5-36
Using Authentication Logs	5-37
Using Configuration History Logs	5-37
Log Subscriptions	5-38
Configuring Log Subscriptions	5-39
Log Levels	5-39
Creating a Log Subscription in the GUI	5-40
Editing Log Subscriptions	5-41
Configuring Global Settings for Logging	5-42
Logging Message Headers	5-43
Configuring Global Settings for Logging via the GUI	5-43
Rolling Over Log Subscriptions	5-44
Rollover By File Size	5-45
Rollover By Time	5-45
Rolling Over Log Subscriptions on Demand	5-46
Viewing Recent Log Entries in the GUI	5-47
Viewing Recent Log Entries in the CLI (tail Command)	5-47
Example	5-48
Configuring Host Keys	5-49

CHAPTER 6

Managing and Monitoring via the CLI 6-1

Reading the Available Components of Monitoring	6-1
Reading the Counters	6-1
Reading the Gauges	6-4
Reading the Rates	6-6
Monitoring Via the CLI	6-6
Monitoring the Email Status	6-7
Example	6-8

Monitoring Detailed Email Status	6-9
Example	6-10
Monitoring the Status of a Mail Host	6-12
Virtual Gateway	6-13
Example	6-14
Determining the Make-up of the Email Queue	6-16
Example	6-17
Displaying Real-time Activity	6-17
Example	6-19
Example	6-20
Monitoring Inbound Email Connections	6-20
Example	6-21
Checking the DNS Status	6-22
Example	6-23
Resetting Email Monitoring Counters	6-23
Example	6-24
Managing the Email Queue	6-24
Deleting Recipients in Queue	6-24
Example	6-25
Bouncing Recipients in Queue	6-26
Example	6-27
Redirecting Messages in Queue	6-28
Example	6-29
Showing Messages Based on Recipient in Queue	6-29
Example	6-29
Suspending Email Delivery	6-31
Example	6-32
Resuming Email Delivery	6-32
Syntax	6-32
Suspending Receiving	6-32
Syntax	6-33
Resuming Receiving	6-33
Syntax	6-33
Resuming Delivery and Receiving	6-34
Syntax	6-34
Scheduling Email for Immediate Delivery	6-34
Syntax	6-34
Pausing the Work Queue	6-35
Locating and Archiving Older Messages	6-37
Syntax	6-37

Syntax	6-37
Tracking Messages Within the System	6-38
SNMP Monitoring	6-39
MIB Files	6-40
Hardware Objects	6-40
Hardware Traps	6-41
SNMP Traps	6-42
CLI Example	6-42

CHAPTER 7**Other Tasks in the GUI 7-1**

The Cisco IronPort Graphical User Interface (GUI)	7-1
Enabling the GUI on an Interface	7-1
Example	7-3
Overview of Remaining Tasks Available in the GUI	7-5
Debugging Mail Flow Using Test Messages: Trace	7-6
GUI example of the Trace Page	7-14
Gathering XML status from the GUI	7-16

CHAPTER 8**Common Administrative Tasks 8-1**

Management of the Cisco IronPort Appliance	8-1
Shutting Down the Cisco IronPort Appliance	8-1
Rebooting the Cisco IronPort Appliance	8-2
Placing the Cisco IronPort Appliance into a Maintenance State	8-2
The suspend and offline Commands	8-4
Resuming from an Offline State	8-4
The resume Command	8-5
Resetting to Factory Defaults	8-5
The resetconfig Command	8-6
Displaying the Version Information for AsyncOS	8-6
Support Commands	8-6
Technical Support	8-7
Remote Access	8-7
Support Request	8-7
Packet Capture	8-8
Working with Feature Keys	8-11
The Feature Keys Page	8-11
Feature Key Settings	8-12
Expired Feature Keys	8-12
Working with User Accounts	8-12

Managing Users	8-14
Adding Users	8-15
Editing Users	8-16
Locking and Unlocking a User Account	8-16
Deleting Users	8-17
Controlling Access to Sensitive Information in Message Tracking	8-18
Changing Your Password	8-18
Additional Commands to Support Multiple Users: who, whoami, and last	8-19
Configuring Restrictive User Account and Password Settings	8-20
External Authentication	8-23
Enabling LDAP Authentication	8-24
Enabling RADIUS Authentication	8-25
Managing Custom User Roles for Delegated Administration	8-26
Account Privileges Page	8-27
Assigning Access Privileges	8-28
Mail Policies and Content Filters	8-29
DLP Policies	8-30
Email Reporting	8-31
Message Tracking	8-32
Trace	8-32
Quarantines	8-32
Encryption Profiles	8-33
Defining a Custom User Role	8-33
Defining a Custom User Role When Adding a User Account	8-33
Updating Responsibilities for a Custom User Role	8-34
Editing a Custom User Role	8-35
Duplicating a Custom User Role	8-35
Deleting a Custom User Role	8-35
Managing the Configuration File	8-36
Managing Multiple Appliances with XML Configuration Files	8-36
Managing Configuration Files via the GUI	8-36
Saving and Exporting the Current Configuration File	8-37
Loading a Configuration File	8-37
Resetting the Current Configuration	8-40
CLI Commands for Configuration Files	8-40
The showconfig, mailconfig, and saveconfig Commands	8-41
The loadconfig Command	8-42
Uploading Configuration Changes via the CLI	8-42
Managing Secure Shell (SSH) Keys	8-44

Disabling SSH1	8-45
Remote SSH Command Execution	8-46

CHAPTER 9

Testing and Troubleshooting 9-1

Debugging Mail Flow Using Test Messages: Trace	9-1
GUI example of the Trace Page	9-10
CLI Example of the trace Command	9-12
Using the Listener to Test the Appliance	9-16
Example	9-17
Troubleshooting the Network	9-20
Strategies to Test the Network Connectivity of the Appliance	9-20
Troubleshooting	9-22
Troubleshooting the Listener	9-26
Troubleshooting Delivery	9-27
Troubleshooting Performance	9-30

INDEX



CHAPTER 1

Managing the Cisco IronPort Email Appliance

The *Cisco IronPort AsyncOS for Email Daily Management Guide* provides instructions for managing and monitoring the Cisco 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, page 1-1](#)
- [How to Use This Guide, page 1-2](#)

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 Cisco 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 Cisco 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, 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 Cisco 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.
- *Cisco 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 Cisco 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 Cisco IronPort appliance as well as the Cisco IronPort Customer Support Portal. For more information, see [Cisco IronPortSupport Community](#), page 1-4.

How to Use This Guide

Use this guide as a resource to learn about how to manage and monitor your Cisco 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 1-2 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 Cisco 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 Cisco IronPort C- or X-Series appliance for email delivery.

How This Book Is Organized

[Chapter 1, “Managing the Cisco 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 Cisco IronPort Spam quarantine.

[Chapter 5, “Logging”](#) describes the logging and log subscription functionality of the Cisco 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 as adding users, managing the configuration file, and managing SSH keys. This chapter also describes how to request technical support, allow Cisco IronPort customer support remote access to your Cisco IronPort appliance, 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
<i>AaBbCc123</i>	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 <i>Cisco IronPort Quickstart Guide</i> . The Cisco IronPort appliance <i>must</i> 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: <i>your_new_password</i> Retype new password: your_new_password

Where to Find More Information

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

Knowledge Base

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

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



Note

If you do not already have an account, click the Register to Log In link on the Cisco IronPort Support page. Generally, only Cisco customers, partners, and employees can access the Knowledge Base.

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

Articles generally fall into one of the following categories:

- **How-To.** These articles explain how to do something with a Cisco 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 a Cisco 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 Cisco IronPort products. For example, a troubleshooting article might provide steps to follow if you are having problems with DNS.

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

Cisco IronPortSupport Community

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

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

<https://supportforums.cisco.com/index.jspa>

Cisco IronPort Customer Support

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

During customer support hours (24 hours per 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 our office hours, please contact Cisco IronPort using one of the following methods:

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

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

Support Portal: <http://cisco.com/web/ironport/index.html>

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

Cisco IronPort Welcomes Your Comments

The Cisco 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-25138-01.



CHAPTER 2

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, 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, page 2-1](#)
- [Email Security Monitor Pages, page 2-2](#)
- [Reporting Overview, page 2-43](#)
- [Managing Reports, page 2-44](#)

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 Cisco IronPort appliance (including quarantines, work queues, and 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 2-20](#)).

**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 Cisco IronPort SenderBase Reputation Service, the Cisco IronPort Anti-Spam scanning service, the Anti-Virus scanning security services, content filters, and 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. For information about generating PDFs in languages other than English, see the ["Notes on Reports" section on page 2-44](#).

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 2-41](#)).

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 (IPv4 and IPv6)
- 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 IPv4 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).

For IPv6 address searches, AsyncOS supports the following formats:

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

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 Cisco IronPort appliance, including an overview of your quarantines and 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 Cisco 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 and non-virus outbreak information based on information available at the Cisco 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 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				Threat Level		
<div>System Status: Online</div> <div>Incoming Messages per hour: 0</div> <div>Messages in Work Queue: 0</div>			Quarantine		% Full	Messages		<div>Outbreak In Last 24 Hours</div> <div>Outbreak Quarantine</div> <div>0.0% <div></div> full 0 messages</div>	
			Policy	0.0%	<div></div>	0			
			Virus	0.0%	<div></div>	0			
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.

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 Outbreak status as reported by the Cisco 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 Outbreak Filters feature on your appliance.



Note

In order for the 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 Threat Level indicator will attempt to use that address. The 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 Cisco IronPort TOC web site. Note that in order for this link to work, your Cisco 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. 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 2-6](#)).

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.

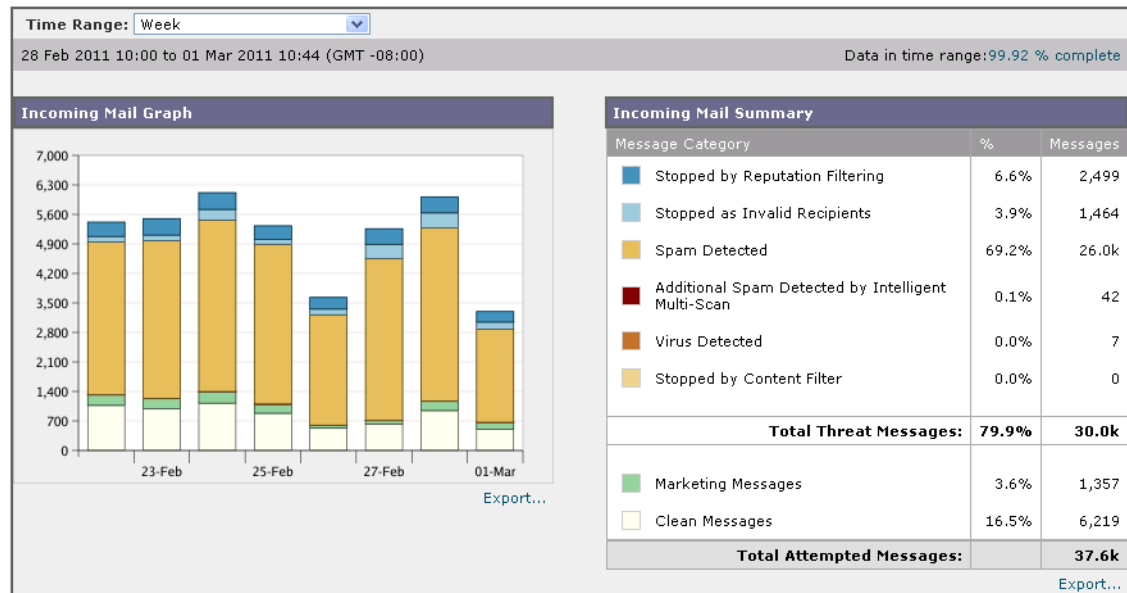
The outgoing graph and summary show similar information for outbound mail.

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 Cisco 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 2-6](#)) 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: 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: 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](#)]

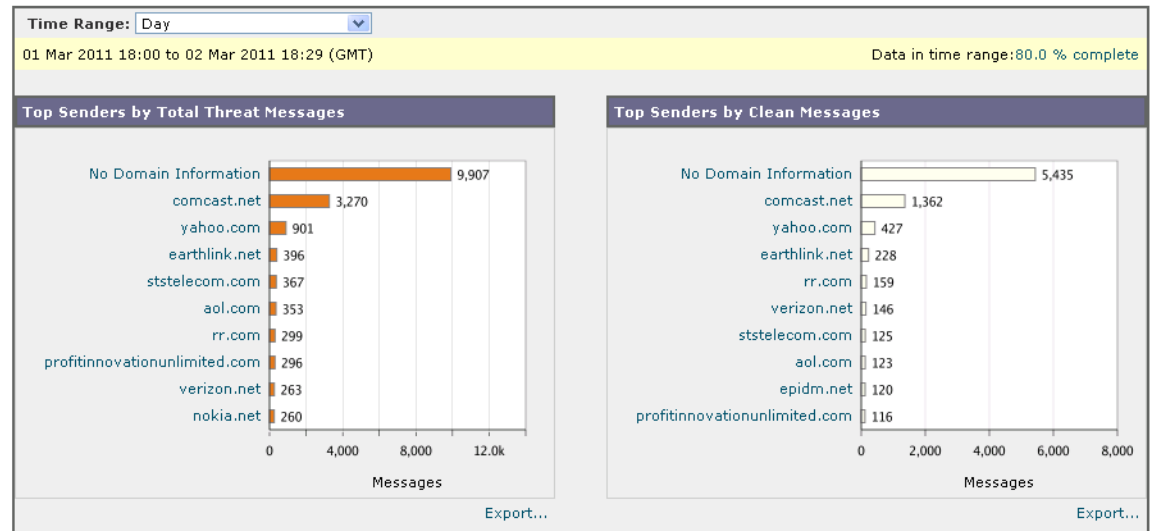
It displays a table (Incoming Mail Details) of the top domains (or IP addresses, or network owners, depending on the view) that have sent mail to all public listeners configured on the appliance. You can monitor the flow of all mail into your gateway. You can click on any domain/IP/network owner to drill 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 2-16](#) 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 Cisco 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 Cisco 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**Figure 2-5 Incoming Mail Details**

Incoming Mail Details									
									Items Displayed 10
Sender Domain	Total Attempted	Stopped by Reputation Filtering ?	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
No Domain Information	15.7k	2,415	0	6,881	196	415	9,907	344	5,435
comcast.net	4,715	687	0	2,217	162	204	3,270	83	1,362
yahoo.com	1,367	222	0	606	18	55	901	39	427
earthlink.net	636	81	0	289	0	26	396	12	228
rr.com	466	78	0	199	0	22	299	8	159
verizon.net	416	60	0	168	28	7	263	7	146
ststelecom.com	498	60	0	221	67	19	367	6	125
aol.com	486	66	0	238	12	37	353	10	123
epidm.net	355	48	0	137	20	23	228	7	120
profitinnovationunlimited.com	428	42	0	254	0	0	296	16	116

See [Incoming Mail Details Listing, page 2-10](#) 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 specify the time range to include in the results shown. Because the data is monitored in real time, information is periodically updated and summarized in the database.

Choose from the time range options in [Table 2-1](#).

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

This time range selected in the GUI	...is defined as:
Hour	the last 60 minutes + up to 5 minutes
Day	the last 24 hours + the last 60 minutes

Table 2-1 Time Ranges Available in the Email Security Monitor Feature (continued)

This time range selected in the GUI	...is defined as:
Week	the last 7 days + the elapsed hours of the current day
30 days	the last 30 days + the elapsed hours of the current day
90 days	the last 90 days + the elapsed hours of the current day
Yesterday	00:00 to 23:59 (midnight to 11:59 PM)
Previous Calendar Month	00:00 of the first day of the month to 23:59 of the last day of the month
Custom Range	the range enclosed by the start date and hour and the end date and hour that you specify

The time range options that you see will differ if you have enabled Centralized Reporting. For details, see information about Centralized Reporting Mode in the “Cisco IronPort M-Series Security Management Appliance” chapter of the *Cisco IronPort AsyncOS for Email Security Configuration Guide*.

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 2-6](#) 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 default Sender Detail 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, stopped by content filter). It also shows the total number of threat messages (messages stopped by reputation or stopped as invalid recipient, spam, and viruses).

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.

Additional columns that you can display are:

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.

Show or hide columns by clicking the Column link at the bottom of the table.

Sort the listing by clicking the column header links. A small triangle beside the column header indicates the column by which the data is currently sorted.

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 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 Cisco 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 2-11](#)).

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 2-16](#).

Reporting Pages Populated with Data: Sender Profile Pages

If you clicked a sender in the Incoming Mail Details table on an 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 an 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

Incoming Mail Details									
Network Owner	Total Attempted	Stopped by Reputation Filtering (?)	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean ▼
Test Inc.	38.0k	6,045	0	16.6k	584	890	24.1k	1,004	12.9k
No Network Owner Information	11.1k	1,536	0	4,743	269	440	6,988	205	3,878
Columns... 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 time range that you specify.
- **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. You can also display the DNS Verified status, SBRS (SenderBase Reputation Score), and Last Sender Group for each sender address in the IP Addresses table by clicking the Columns link at the bottom of that table. You can also hide any columns in that table.

From a network owner profile page, you can display Connections Rejected, Connections Accepted, and Stopped by Recipient Throttling information for each domain in the Domains table by clicking the Columns link at the bottom of that table. You can also hide any columns in that table.

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.

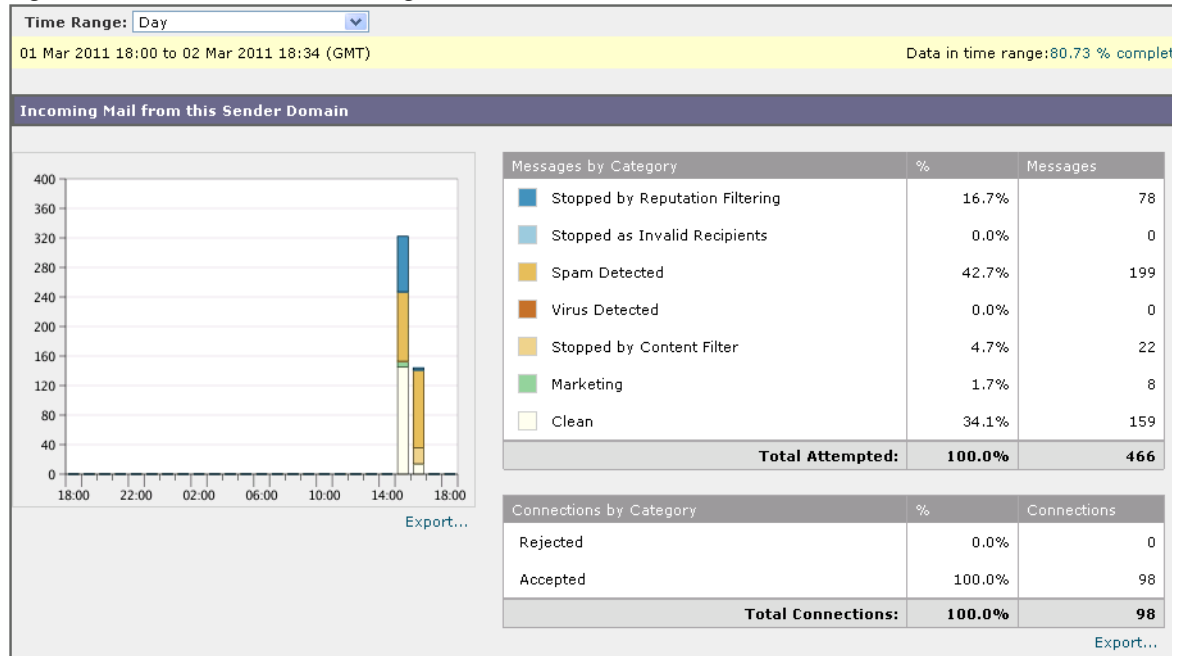
Figure 2-7 Current Information for Network Owner

Current Information for EXAMPLE.COM	
Current Information from SenderBase	Sender Group Information
<p>Network Owner Category: NSP</p> <p>Daily Magnitude: 7.8</p> <p>Monthly Magnitude: 7.5</p> <p>Days Since First Message from this Network Owner: -- days</p> <p>Number of Domains Associated with this Network Owner: 1,928</p> <p>Number of IP Addresses Used to Send Mail: 3.7M</p>	<p>Last Sender Group: UNKNOWNLIST</p>
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 2-11](#).

Figure 2-8 Domain Profile Page (1 of 2)**Figure 2-9 Domain Profile Page (2 of 2)**

IP Addresses										
										Items Displayed <input type="text" value="10"/>
Sender IP Address	Hostname	Total Attempted	Stopped by Reputation Filtering ?	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
24.29.109.6	...tp-02.rdc-nyc.rr.com	26	6	0	2	0	0	8	1	17
24.93.47.42	ms-smtp-03.texas.rr.com	26	6	0	6	0	0	12	0	14
65.32.5.134	...p-04.tampabay.rr.com	117	3	0	79	0	21	103	0	14
24.24.2.58	ms-smtp-04.nyroc.rr.com	13	3	0	1	0	0	4	0	9
24.93.40.211	austtx-mx-04.mgw.rr.com	13	3	0	1	0	0	4	0	9
65.32.5.135	...p-05.tampabay.rr.com	26	6	0	11	0	0	17	0	9
66.75.162.134	ms-smtp-02.socal.rr.com	13	3	0	2	0	0	5	0	8
24.24.2.57	ms-smtp-03.nyroc.rr.com	13	3	0	2	0	0	5	1	7
65.24.0.113	...0-113.ohiordc.rr.com	13	3	0	3	0	0	6	0	7
69.205.138.18	...8-18.stny.res.rr.com	13	3	0	2	0	0	5	1	7

Columns... | Export...

Figure 2-10 Network Owner Profile Page (1 of 2)
Sender Profile: Test Inc.

Printable (PDF)

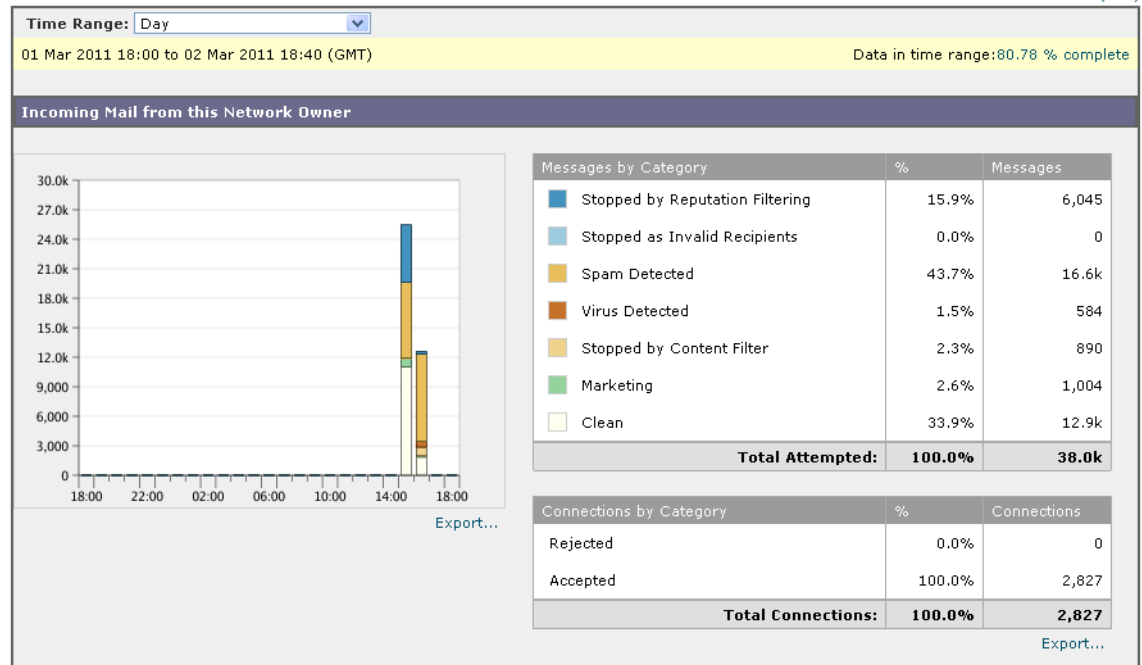
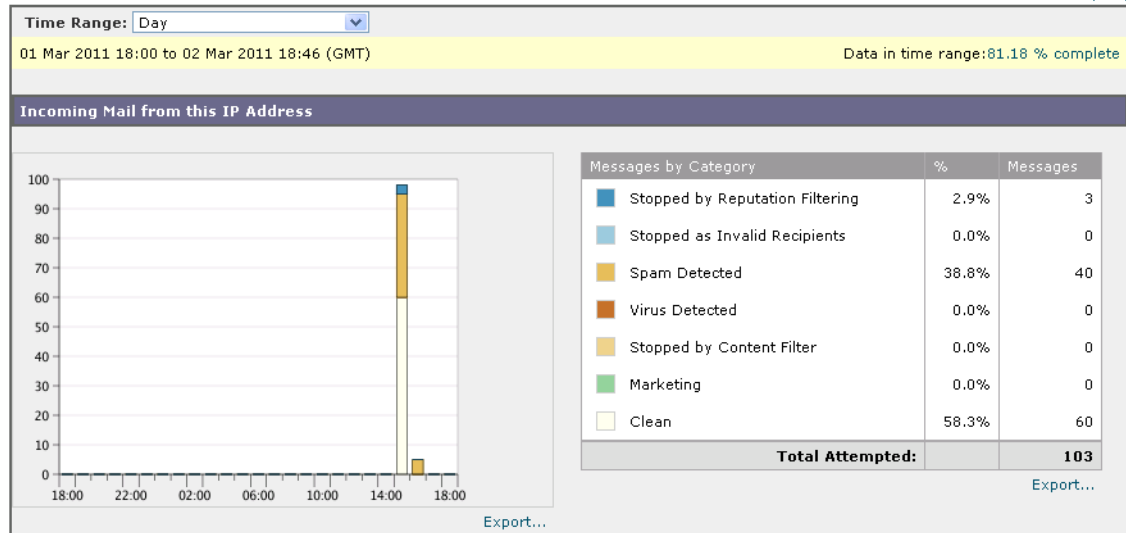


Figure 2-11 Network Owner Profile Page (2 of 2)

Domains Items Displayed

Sender Domain	Total Attempted	Stopped by Reputation Filtering (?)	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
No Domain Information	12.5k	2,001	0	5,574	152	310	7,727	295	4,428
comcast.net	4,361	684	0	2,175	113	140	2,972	83	1,306
yahoo.com	1,094	186	0	522	0	51	708	26	360
earthlink.net	604	81	0	284	0	25	365	12	227
rr.com	441	78	0	196	0	21	274	8	159
verizon.net	402	60	0	163	28	7	251	7	144
ststelecom.com	470	60	0	213	67	19	340	6	124
aol.com	441	66	0	231	12	36	309	10	122
pacificrack.com	335	57	0	157	0	21	214	10	111
profitinnovationunlimited.com	421	42	0	253	0	0	295	16	110

Columns... | Export...

Figure 2-12 IP Address Profile Page (1 of 2)**Sender Profile: 209.86.89.68 - elasmtp-masked.atl.sa.earthlink.net**[Printable \(PDF\)](#)**Figure 2-13 IP Address Profile Page (2 of 2)**

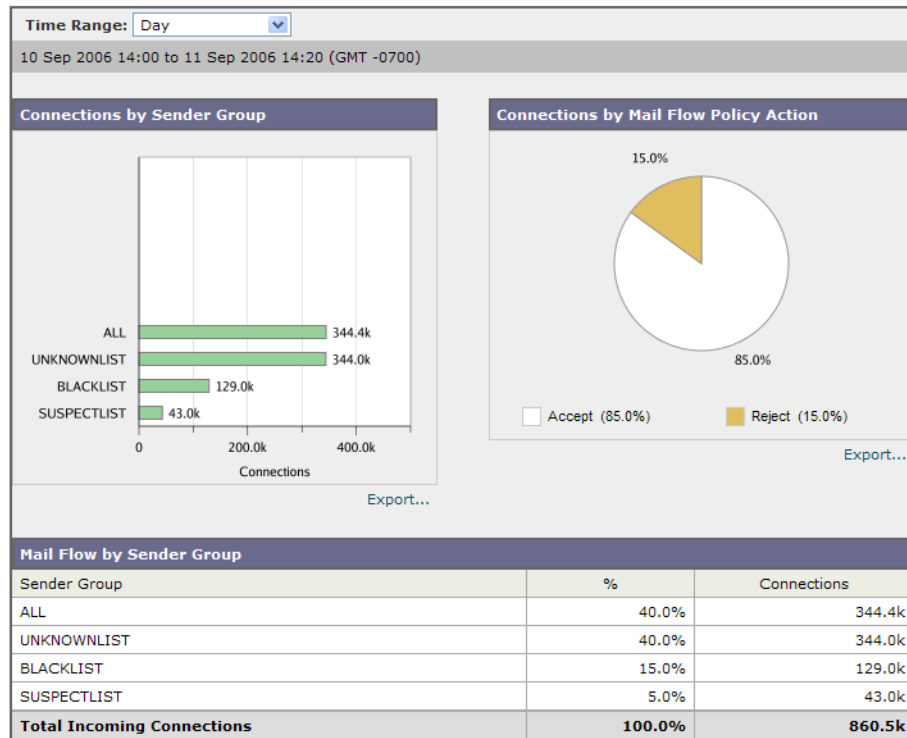
Current Information for 65.32.5.134		
Current Information from SenderBase	Sender Group Information	Network Information
SenderBase Reputation Score (SBRS): 3 Bonded Sender Status: 0 Daily Magnitude: 5.1 Monthly Magnitude: 4.6 CIDR Range: 14 Average Magnitude: 5.8	Last Sender Group: ALL DNS Verified: Yes	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
Sender Groups

Printable (PDF)



Outgoing Destinations

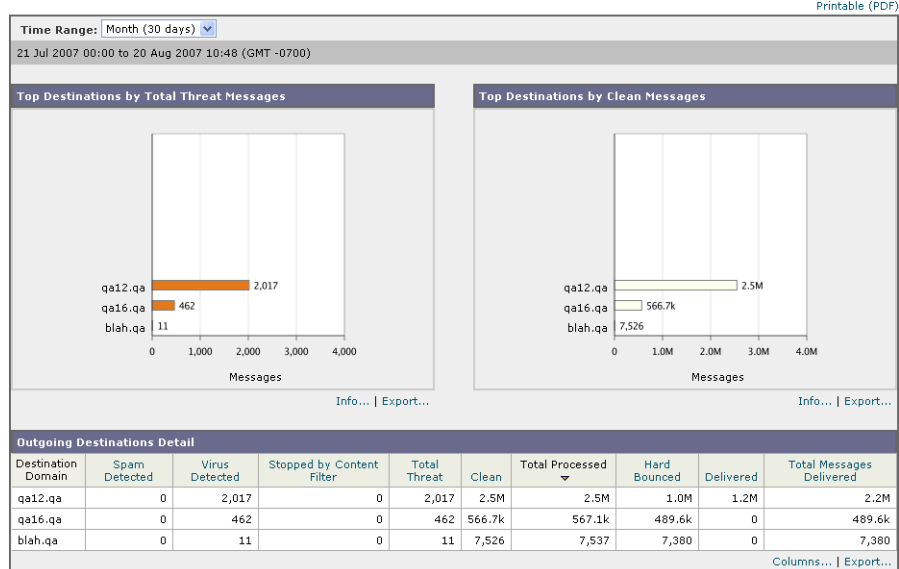
The Outgoing Destinations page provides information about the domains your company sends mail to. The page consists of two section. The top half of the page consists of graphs depicting the top destinations by outgoing threat messages and top destinations by outgoing clean messages on the top half of 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, such as an hour, a week, or a custom range. 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 Cisco 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



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 to 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 graph 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).



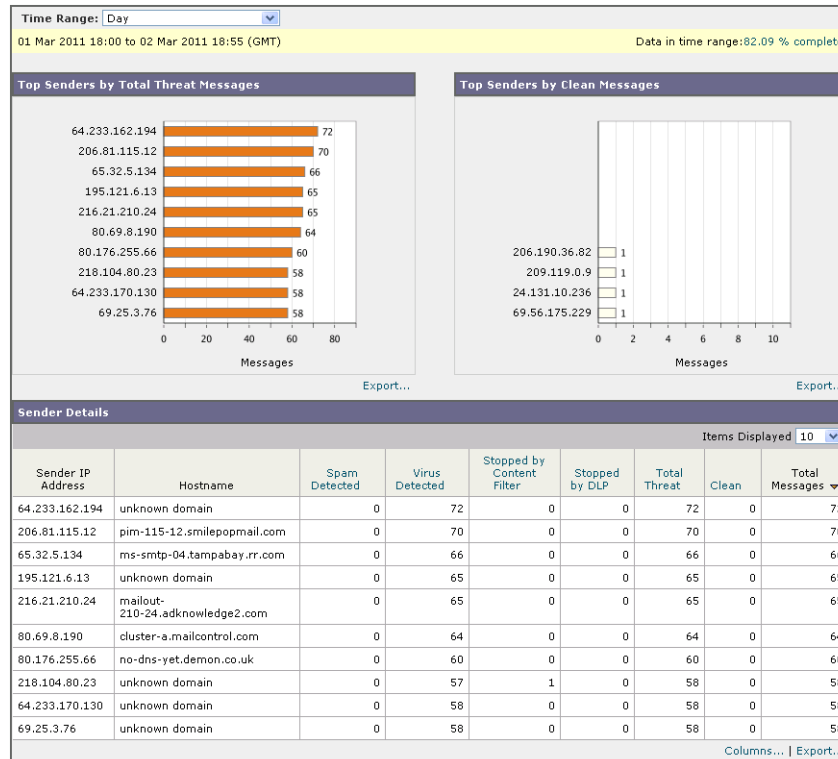
Note

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, such as an hour, a week, or a custom range. 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)*

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 6-34](#).

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

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

Delivery Status Details				
Ordered IP Addresses				
Preference	IP Address	Recipients	Limit	Rate Limiting Minutes Remaining
10	172.21.116.1	N/A	N/A	N/A

Counters	
Queue	
Soft Bounced Events	0
Completion	
DNS Hard Bounces	0
SXX Hard Bounces	0
Filter Hard Bounces	0
Expired Hard Bounces	5,094
Other Hard Bounces	0
Hard Bounced Recipients:	5,094
Delivered Recipients:	0
Deleted Recipients:	0
Completed Recipients:	5,094

Gauges	
Queue	
Unattempted Recipients	2,675
Attempted Recipients	0
Active Recipients:	2,675
Connections	
Current Outgoing Connections	0
Pending Outgoing Connections	0
Throttle	
Current Recipients	0
Recipient Limit	0
Minutes Remaining	60

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.

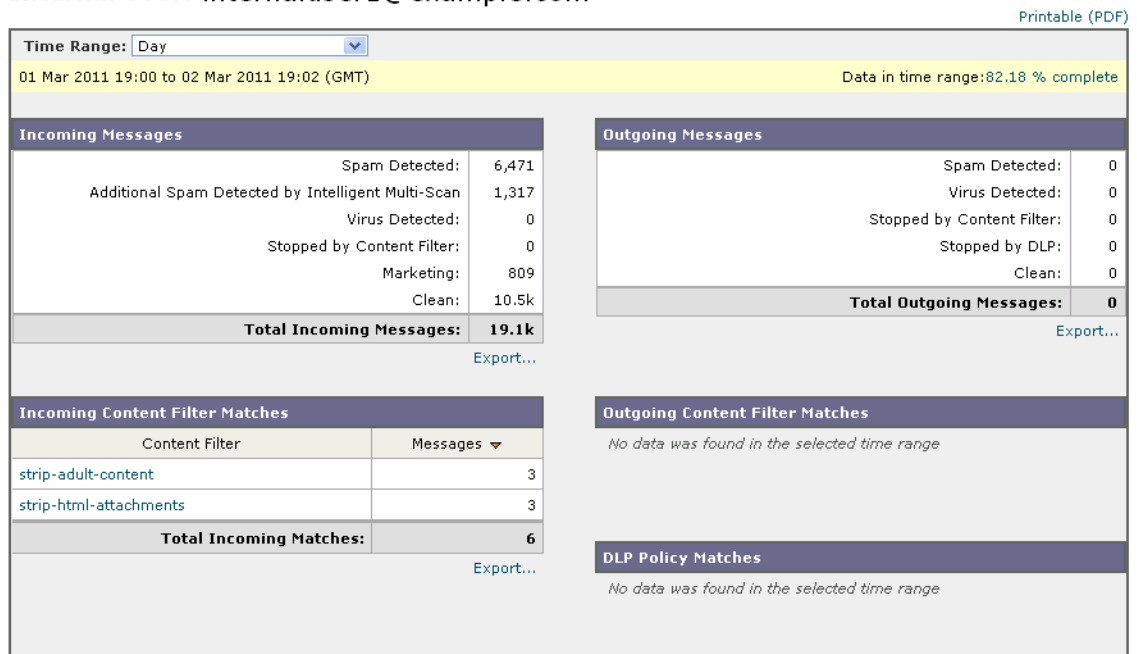
Note that some outbound mail (like bounces) have a null sender. They are counted under outbound and “unknown.”

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
Internal User: internaluser1@example.com

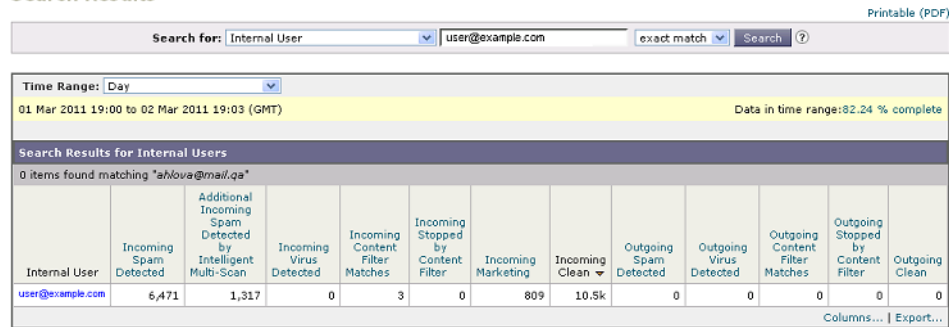


Click on a content filter name to view detailed information for that filter in the corresponding content filter information page (see [The Content Filters Page, page 2-25](#)). You can use this method to get a list of users who also sent or received mail that matched that particular content filter.

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 Cisco 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, such as an hour, a week, or a custom range. 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. For information about generating PDFs in languages other than English, see the “Notes on Reports” section on page 2-44.

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

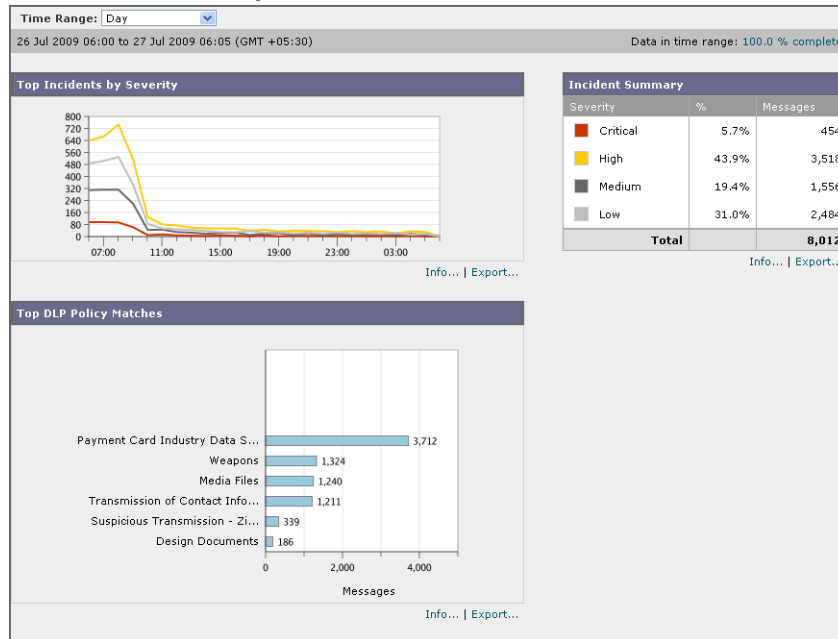


Figure 2-22 DLP Incident Details

DLP Incident Details								
DLP Policy	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
Payment Card Industry Data Security Standard (PCI-DSS)	1,391	906	961	454	3,712	0	0	0
Weapons	902	422	0	0	1,324	0	0	0
Media Files	0	0	1,240	0	1,240	0	0	0
Transmission of Contact Information	191	228	792	0	1,211	0	0	0
Suspicious Transmission - Zip Files	0	0	339	0	339	0	339	0
Design Documents	0	0	186	0	186	0	0	0

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 the number of messages 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

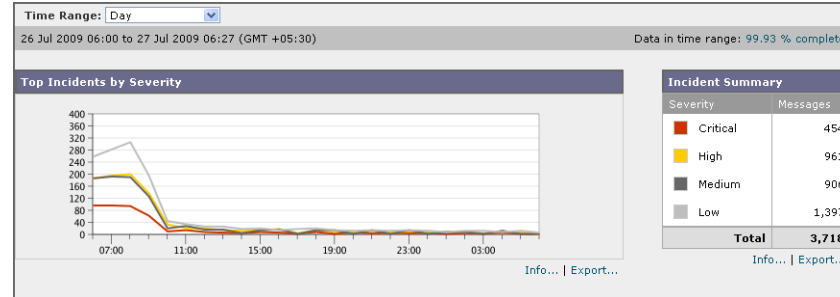


Figure 2-24 DLP Policy Incidents by Sender

Incidents by Sender								
Items Displayed 10								
Sender	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
user@test.com	698	453	480	227	1,858	0	0	0
testuserTP1@test.com	171	0	0	57	228	0	0	0
testuseridentities@test.com	114	0	0	0	114	0	0	0
testuserentco@test.com	0	112	0	0	112	0	0	0
testuser200cc@test.com	0	0	0	57	57	0	0	0
testuser25cc@test.com	0	0	57	0	57	0	0	0
testusercontact_IPAddr_visa@test.com	0	0	57	0	57	0	0	0
testusercontact_visa@test.com	0	0	57	0	57	0	0	0
testuserCreditcard_sev_high@test.com	0	0	57	0	57	0	0	0
testuserCritical_violation_DL@test.com	0	57	0	0	57	0	0	0

Clicking on the sender name opens up the Internal Users page. See [The Internal Users Page, page 2-21](#) 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.

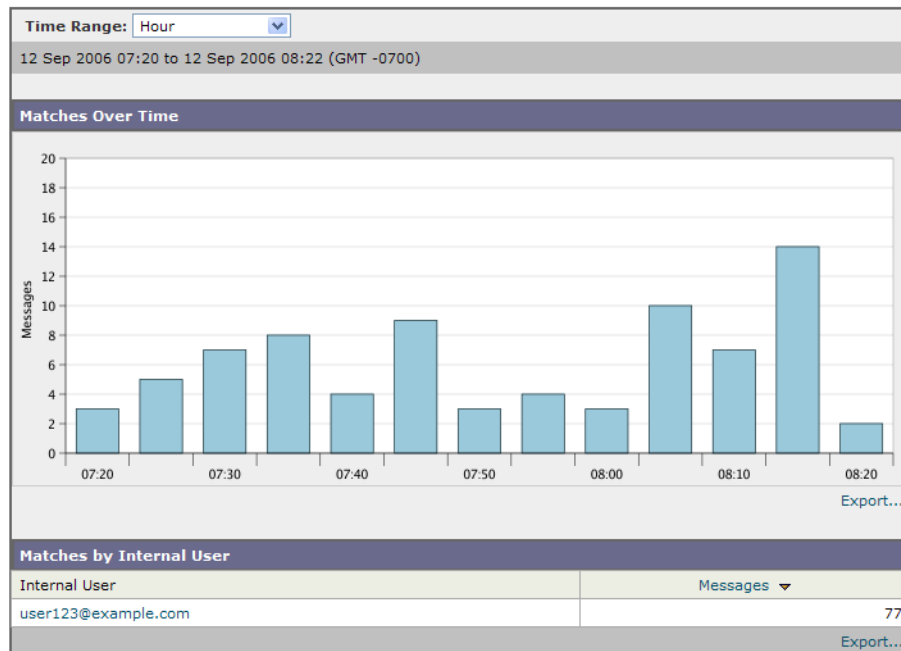
Content Filter Details

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 2-22).

Figure 2-25 *Content Filters Page*
Outgoing Content Filter: free_stuff

[Printable \(PDF\)](#)



The Outbreak Filters Page

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

The Threats By Type section shows the different types of threat messages received by the appliance. The Threat Summary section shows a breakdown of the messages by Virus, Phish, and Scam.

The Past Year Outbreak Summary lists global as well as local outbreaks over the past year, allowing you to compare local network trends to global trends. The listing of global outbreaks is a superset of all outbreaks, both viral and non-viral, whereas local outbreaks are limited to virus outbreaks that have affected your Cisco IronPort appliance. Local outbreak data does not include non-viral threats. Global outbreak data represents all outbreaks detected by the Cisco IronPort Threat Operations Center which exceeded the currently configured threshold for the outbreak quarantine. Local outbreak data represents all virus outbreaks detected on this appliance which exceeded the currently configured threshold for the outbreak quarantine. The Total Local Protection Time is always based on the difference between when each virus outbreak was detected by the Cisco IronPort Threat Operations Center and the release of an anti-virus signature by a major vendor. Note that not every global outbreak affects your Cisco 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 Outbreak Filters quarantining, and is a useful gauge of how many potential threat messages Outbreak Filters are catching. Quarantined messages are counted at time of release. Typically, messages will be quarantined before anti-virus and anti-spam rules are available. When released, they will be scanned by the anti-virus and anti-spam software and determined to be positive or clean. Because of the dynamic nature of 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 Threat Details listing displays information about specific outbreaks, including the threat category (virus, scam, or phishing), threat name, a description of the threat, and the number of messages identified. For virus outbreaks, the Past Year Virus Outbreaks include the Outbreak name and ID, time and date a virus outbreak was first seen globally, the protection time provided by 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.

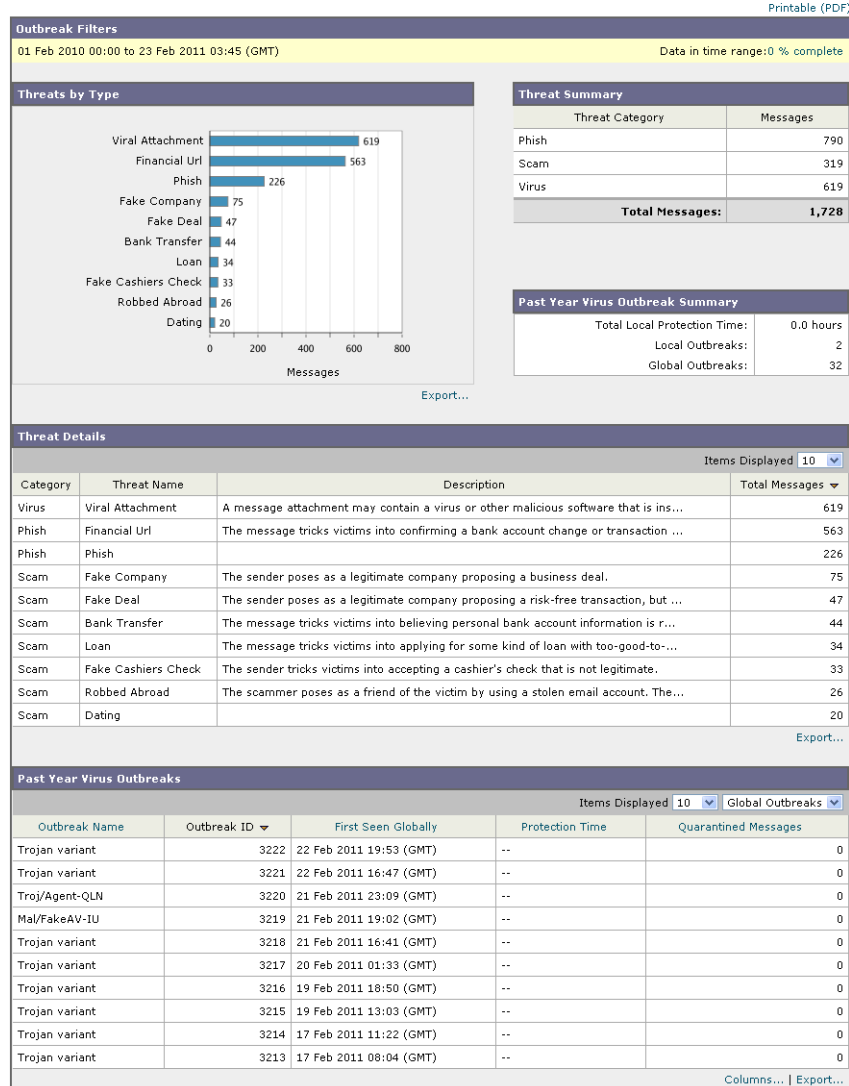
The First Seen Globally time is determined by the Cisco IronPort Threat Operations Center, based on data from SenderBase, the world's largest email and web traffic monitoring network. The Protection Time is based on the difference between when each threat was detected by the Cisco IronPort Threat Operations 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 Outbreak Filters page, you can answer questions like:

- How many messages are being quarantined and what type of threats were they?
- How much lead time has the Outbreak Filter feature been providing for virus outbreaks?
- How do my local virus outbreaks compare to the global outbreaks?

Figure 2-26 **Outbreak Filters Page**
Outbreak Filters



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 Cisco 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.

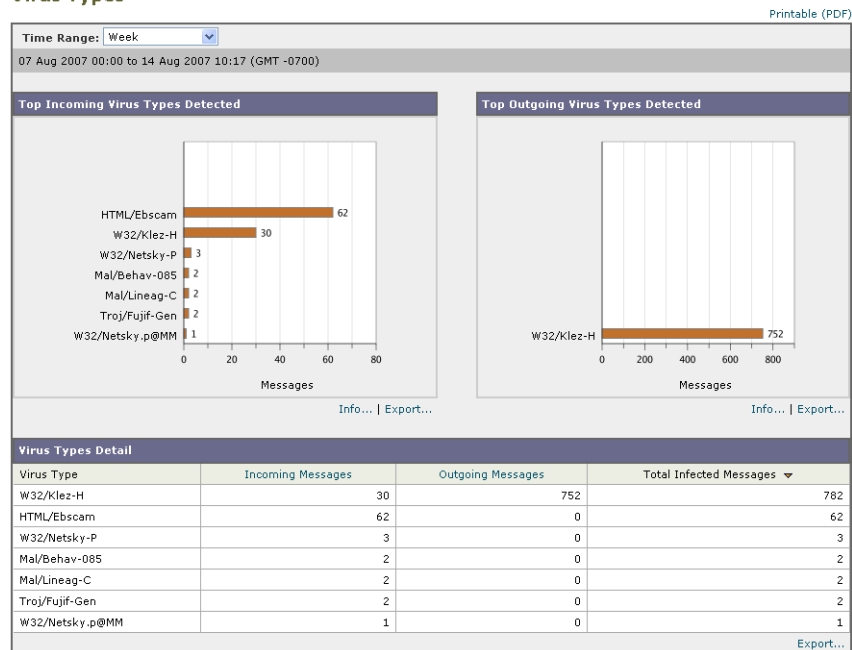
If you run multiple virus scanning engines, the Virus Types page includes results from all enabled virus scanning engines. The name of the virus displayed on the page is a name determined by the virus scanning engines. If more than one scanning engine detects a virus, it is possible to have more than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



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:

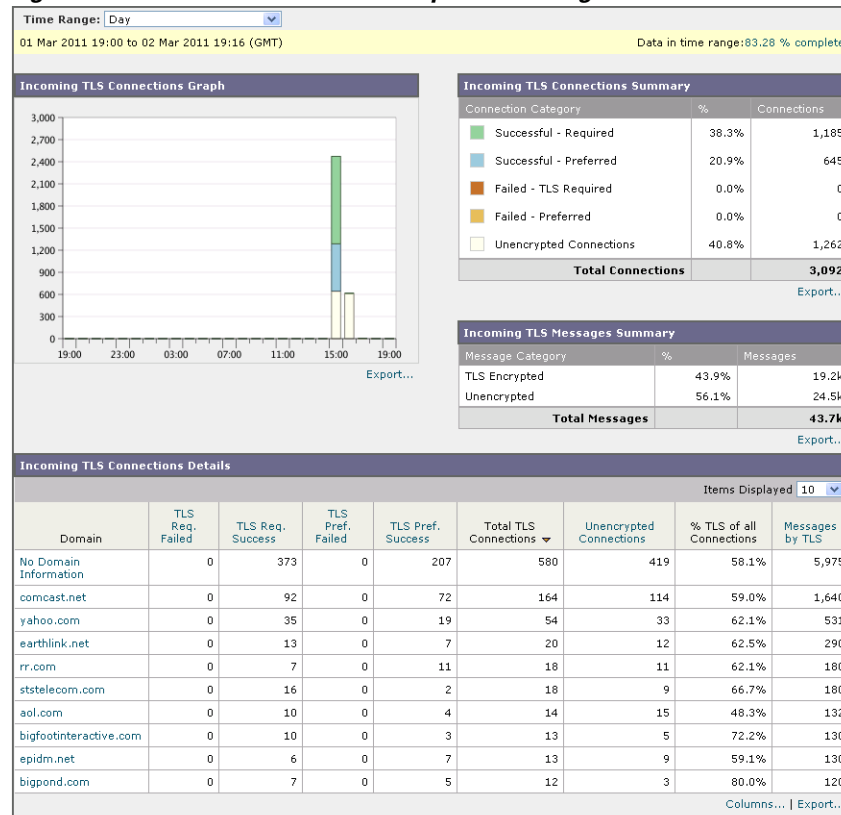
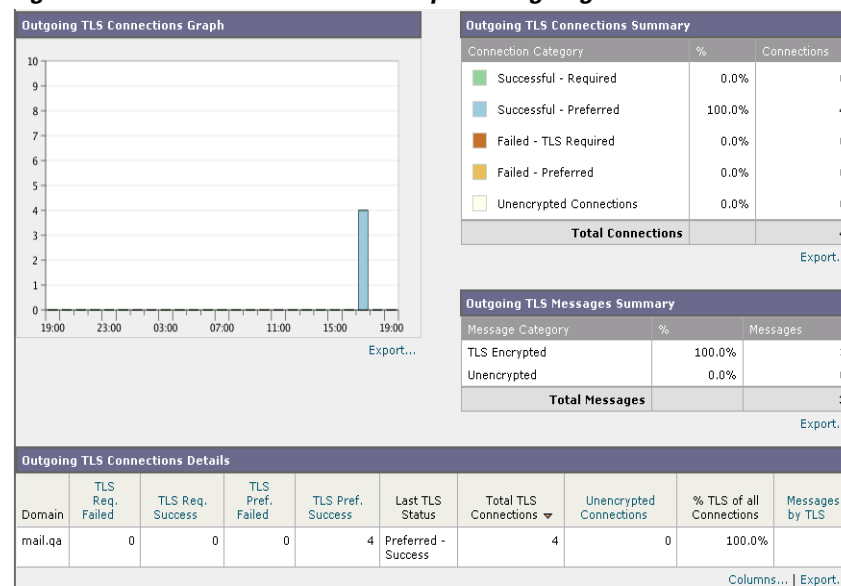
- Overall, what portion of incoming and outgoing connections use TLS?
- What partners do I have successful TLS connections with?
- What partners do I have unsuccessful TLS connections with?
- What partners have issue with their TLS certificates?

- What percent of overall mail with a partner uses TLS?

The TLS Connections page is divided into a section for incoming connections and a section for outgoing connections. Each section includes a graph, summaries, and a table with details.

The graph displays a view of incoming or outgoing TLS-encrypted and non-encrypted connections over the time range you specify. 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 graphs distinguish between connections in which TLS was required and connections in which TLS was merely preferred.

The table displays details for domains sending or receiving encrypted messages. For each domain, you can view the number of required and preferred TLS connections that were successful and that failed, the total number of TLS connections attempted (whether successful or failed), and the total number of unencrypted connections. You can also view the percentage of all connections in which TLS was attempted, and the total number of encrypted messages sent successfully, regardless of whether TLS was preferred or required. You can show or hide columns by clicking the Columns link at the bottom of this table.

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

Rate Limits Page

Rate Limiting by envelope sender allows you to limit the number of email messages per time interval

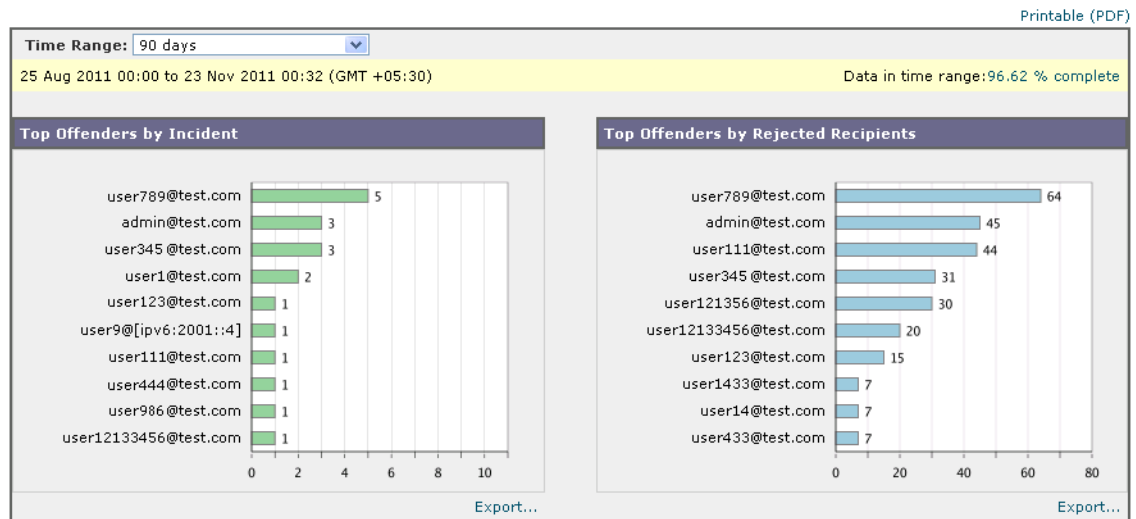
from an individual sender, based on the mail-from address. The Rate Limits report allows you to quickly identify individual senders of large numbers of messages. Use this report to help you to:

- Control spam from internal user accounts, for example in cases when a user's credentials are compromised and the account is used to send spam in bulk.
- Identify compromised user accounts.
- Limit out-of-control applications that use email for notifications, alerts, automated statements, etc.
- Avoid damaging your organization's online reputation and the attendant hassles resulting from this situation

Rate Limiting is configured in Mail Policies > Mail Flow Policies. For more information on rate limiting, see the “Configuring the Gateway to Receive Email” chapter in the *AsyncOS for Email Configuration Guide*.

Figure 2-30 Rate Limits Page

Rate Limits



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 a Cisco 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 Cisco 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 2-34](#) and [System Capacity-Outgoing Mail, page 2-35](#).
- **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 2-33](#).
- **Resource Conservation Mode:** When a Cisco 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 Cisco 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 Cisco 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.

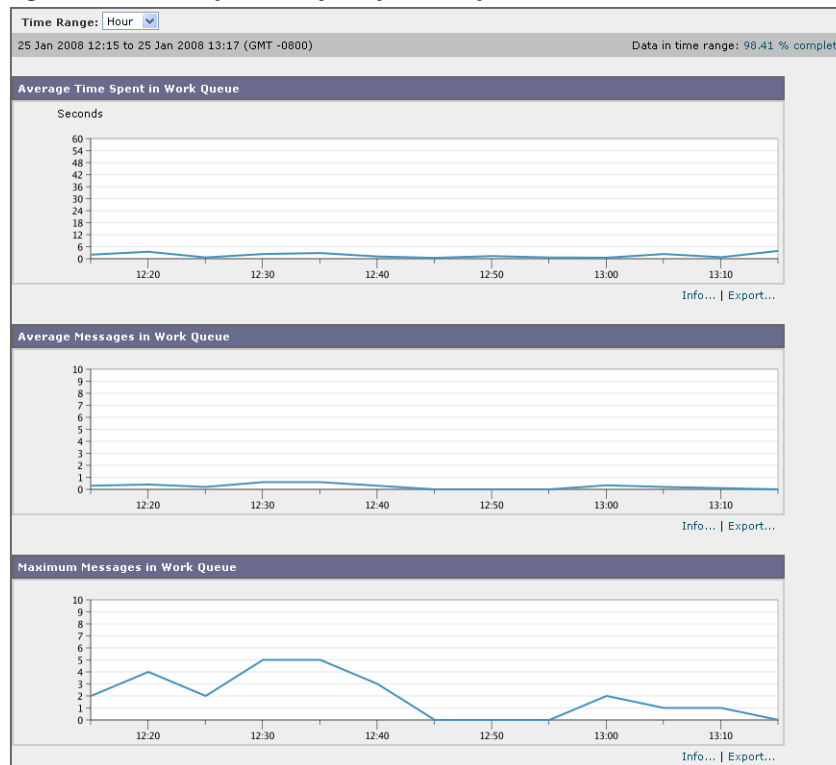


Note

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 2-31 System Capacity - Workqueue

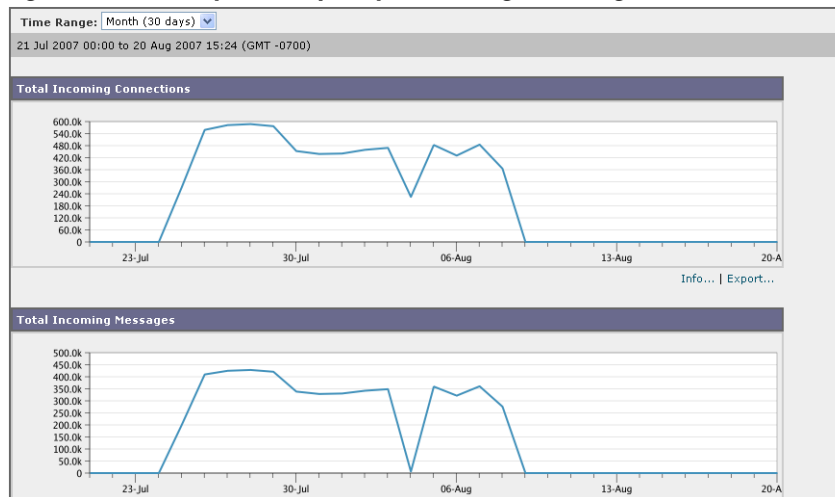
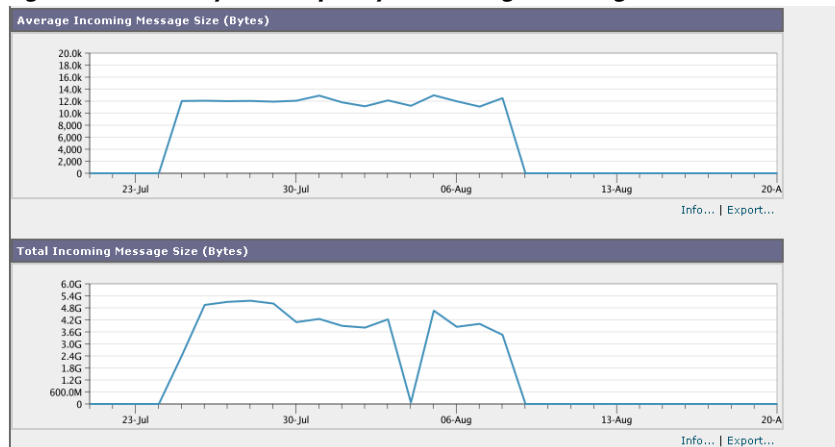
System Capacity- Incoming Mail

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 to the time range that you specify. 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.



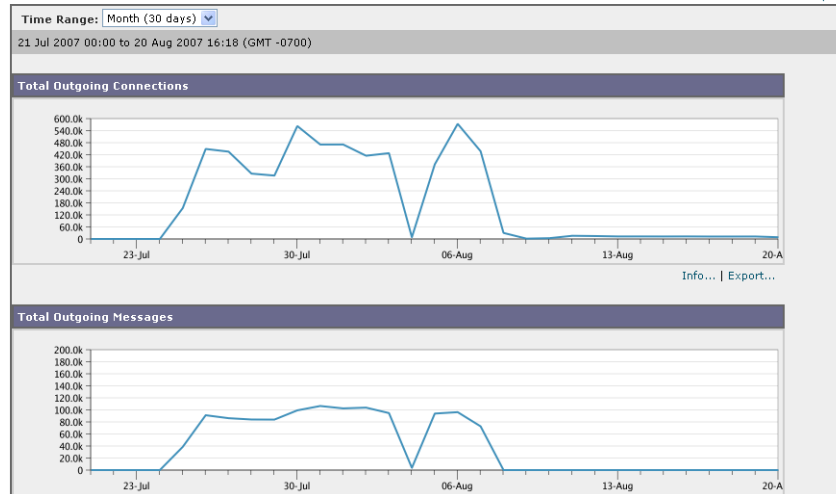
Note

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

Figure 2-32 System Capacity - Incoming Mail (Page 1 of 2)**Figure 2-33 System Capacity - Incoming Mail (Page 2 of 2)**

System Capacity-Outgoing Mail

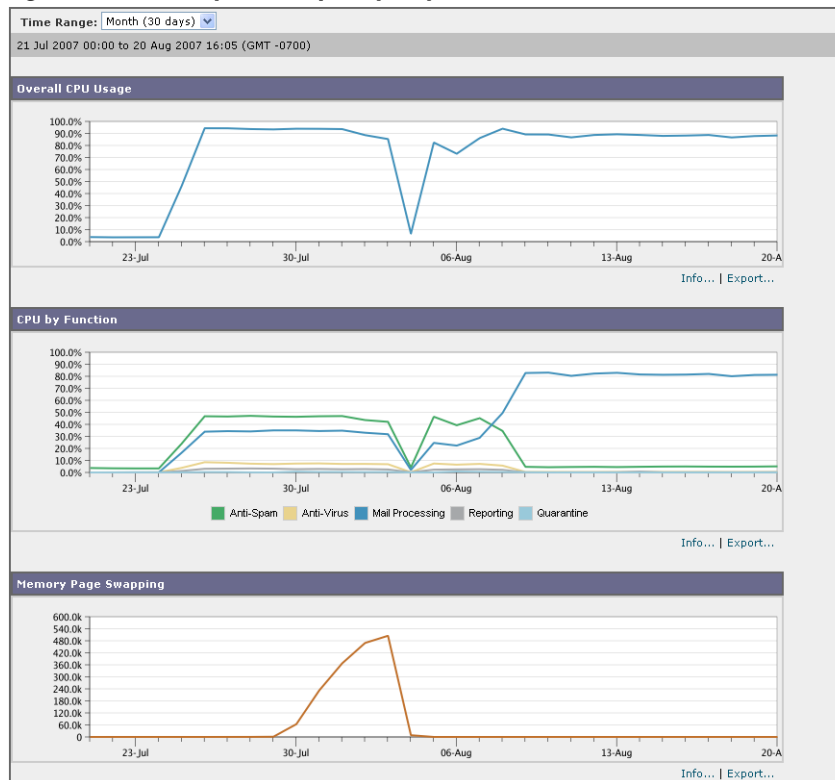
The outgoing mail page shows outgoing connections, the total number of outgoing messages, the average message size, and the total outgoing message size. You can limit the results to the time range that you specify. It is important to have an understanding of the trends of normal message volume and spikes 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 2-34 System Capacity - Outgoing Mail (page 1 of 2)**System Capacity**[[Workqueue](#) | [Incoming Mail](#) | **[Outgoing Mail](#)** | [System Load](#) | [All](#)][Printable \(PDF\)](#)**Figure 2-35 System Capacity - Outgoing Mail (page 2 of 2)**

System Capacity-System Load

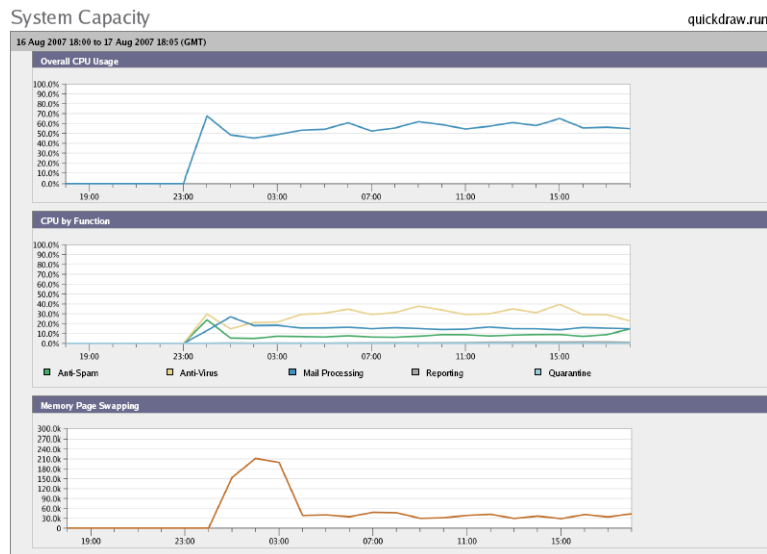
The system load report shows the overall CPU usage on your Cisco IronPort appliance. AsyncOS is optimized to use idle CPU resources to improve message throughput. High CPU usage may not indicate a system capacity problem. If the high CPU usage is coupled with consistent, high-volume memory page swapping, 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 2-36 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 C150/C160 appliances). For example, [Figure 2-37](#) shows a system that consistently swaps memory in high volumes. To improve performance, you may need to add Cisco IronPort appliances to your network or tune your configuration to ensure maximum throughput.

Figure 2-37 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). For information about generating PDFs in languages other than English, see the [“Notes on Reports”](#) section on page 2-44.

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 2-4](#))
- 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 Cisco IronPort AsyncOS operating system installed.
- The installation date of the Cisco IronPort AsyncOS operating system.
- The serial number of the system to which you are connected.

This information is useful if you are contacting Cisco IronPort Customer Support. (See [Cisco IronPort Customer Support, page 1-4.](#))

Figure 2-38 System Status

System Status	
Mail System Status	Version Information
System Status: Online	Model: C600
Status as of: 26 Oct 2006 09:15 (GMT -0700)	Operating System: 5.0.0-132
Up Since: 25 Oct 2006 23:18 (GMT -0700) (9h 57m 36s)	Build Date: 24 Oct 2006 00:00 (GMT -0700)
Oldest Message: 3 days 33 mins 40 secs	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 Cisco IronPort Anti-Spam scanning engine and Outbreak Filters processes.

- General Resource Utilization
- Logging Disk Utilization

Figure 2-39 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%
Active Messages in Work Queue	683	Anti-Virus	5.0%
Active Messages in Quarantine	28.7k	Context Adaptive Scanning Engine (CASE)	47.0%
Active Destination Objects in Memory	11.7k	Total CPU Utilization:	99.0%
Active Recipients in Queue		General Resource Utilization	
Unattempted	8,611	RAM Utilization	20.0%
Attempted	28	Disk I/O Utilization	14.0%
Total Active Recipients:	8,639	Logging Disk Utilization	
Queue Space		Logging Disk Utilization	8.0%
Queue Space Used by Quarantine	536957K	Logging Disk Available	150G
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 2-40 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 [Working with User Accounts, page 8-12](#).

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 6-23](#).

- Mail Handling Events
- Completion Events

- Domain Key Events
- DNS Status

Figure 2-41 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 2-43](#).

- **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 Outbreaks report.
- The CSV 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 2-43](#)) and keys (see [Keys, page 2-43](#)) 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 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. 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 Cisco 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
- Outbreak Filters
- 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.



Note

To generate PDFs in Chinese, Japanese, or Korean on Windows computers, you must also download the applicable Font Pack from Adobe.com and install it on your local computer.

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 Outbreak Filters. 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 a time at which to run the report. Regardless of when you run a report, it will only include data for the time period that you specify, for example the past 3 days or the previous calendar month. Note that a daily report scheduled to run at 1AM will contain data for the previous day, midnight to midnight.

Your Cisco 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 2-42 Adding a Scheduled Report

Add Scheduled Report

- 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 2-43](#).
- 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 Outbreak Filters 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.
- For information about generating PDFs in languages other than English, see the [“Notes on Reports” section on page 2-44](#).
- **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 delivery 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 2-43 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 2-44 Generate Report Dialog

Generate Report

Report Type:	Select report type...
Title:	
Time Range To Include:	Previous 7 calendar days
Format:	<input checked="" type="radio"/> PDF <input type="radio"/> CSV ?
Delivery Options:	<input checked="" type="checkbox"/> Archive <input type="checkbox"/> Email now to recipients: Separate multiple addresses with commas.
Report Language:	English/United States [en-us]

- 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 2-43](#).

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

If you create a custom range, the range will appear as a link. To modify the range, click the link.

- 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.

For information about generating PDFs in languages other than English, see the [“Notes on Reports”](#) section on page 2-44.

- **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. Specify any report options.

- Step 5** Select whether to archive the report (if so, the report will shown on the Archived Reports page).

- Step 6** Specify whether to email the report and to which email addresses to send the report.

- Step 7** Click **Deliver this Report** to generate the report and deliver it to recipients or archive it.

Step 8 Commit your changes.



CHAPTER 3

Tracking Email Messages

This chapter contains the following sections:

- [Tracking Service Overview, page 3-1](#)
- [Enabling and Disabling Local Message Tracking, page 3-2](#)
- [Understanding Tracking Query Setup, page 3-3](#)
- [Running a Search Query, page 3-5](#)
- [Understanding Tracking Query Results, page 3-6](#)

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 Cisco 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 3-2](#).

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).
- **Attachment name:** You can search for messages based on the attachment name in the Envelope information fields (envelope senders or envelope recipients). Messages that contain at least one attachment with the queried name will appear in the search results.

Some attachments may not be tracked. For performance reasons, scanning of attachment names occurs only as part of other scanning operations, for example message or content filtering, DLP, or disclaimer stamping. Attachment names are available only for messages that pass through body scanning while the attachment is still attached. Some examples when an attachment name will not appear include (but are not limited to):

- if the system only uses content filters, and a message is dropped or its attachment is stripped by anti-spam or anti-virus filters
- if message splintering policies strip the attachment from some messages before body scanning occurs.

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.



Note

In order to search for and display attachment names in Message Tracking and view attachment names in log files, you must configure and enable at least one body scanning process, such as a message filter or content filter. For more information, see the “Email Security Manager” chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* and corresponding sections in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*.

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, attachment name, 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*
Message Tracking

The screenshot shows a web-based search interface for email messages. At the top, it says 'Search' and 'Available Time Range: 13 Aug 2007 14:52 to 14 Aug 2007 05:52 (GMT -0700)' with a status 'Data in time range: 100.0% complete'. Below this are four search criteria sections: 'Envelope Sender: (?)', 'Envelope Recipient: (?)', 'Subject:', and 'Date and Time Range: (?)'. Each section has a 'Begins With' dropdown menu and a text input field. The 'Date and Time Range' section also includes 'Start Date:', 'Time:', 'and', 'End Date:', and 'Time:' fields. At the bottom left is a 'Clear' button, and at the bottom right is a 'Search' button. A link labeled 'Advanced' is also present, with the text 'Search messages using advanced criteria' below it.

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

Figure 3-3 Advanced Options for Tracking Message Tracking

Search

Available Time Range: 22 Feb 2011 17:57 to 28 Feb 2011 18:45 (GMT) Data in time range: 100.0% complete

Envelope Sender: ?

Begins With

Envelope Recipient: ?

Begins With

Subject:

Begins With

Message Received:

Last Day

Last Week

Custom Range

Start Date:

Time:

and

End Date:

Time:

(GMT +00:00)

02/27/2011

18:00

02/28/2011

18:47

Advanced

Sender IP Address:

Search rejected connections only

Search messages

Attachment Name:

Begins With

Message Event:

Selecting multiple events will expand your search to include messages that match each event type. However, combining an event type with other search criteria will narrow the search.

Virus Positive

Hard bounced

Spam Positive

Soft bounced

Suspect Spam

Quarantined as Spam

Delivered

Currently in Outbreak Quarantine

DLP Violations

Message ID Header:

IronPort MID:

Query Settings: ?

Query timeout:

1 minute

Max. results returned:

250

Clear

Search



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”).

By default, only administrators can view matched content when running searches for DLP violations. To allow other users, including delegated administrators, to view this content, enable the DLP Tracking Privileges through the **System Administration > Users** page. See [Controlling Access to Sensitive Information in Message Tracking](#), page 8-18 for more information.

- **Message-ID Header and MID:** Enter a text string for the “Message-ID:” header, the IronPort message ID (MID), or both.
- **Attachment Name:** Select Begins With, Is, or Contains, and enter an ASCII or Unicode text string for one Attachment Name to find. Leading and trailing spaces are not stripped from the text you enter.

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 3-3.

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

Results				Items per page: 20
Displaying 1 — 3 of 3 items.				
1	13 Aug 2011 13:55:41 (GMT -0700)	MID: 13	HOST: elroy.run (172.19.0.11)	Show Details
SENDER: jsmith@smith.com				
RECIPIENT: joe@mail.qa				
SUBJECT: Test7				
LAST STATE: N/A				
attachment.jpg, allmystuff.doc				
2	13 Aug 2011 13:44:29 (GMT -0700)	MID: 11	HOST: elroy.run (172.19.0.11)	Show Details
SENDER: jsmith@smith.com				
RECIPIENT: joeshmoe@ironport.com				
SUBJECT: Test2				
LAST STATE: N/A				
3	13 Aug 2011 13:42:18 (GMT -0700)	MID: 10	HOST: elroy.run (172.19.0.11)	Show Details
SENDER: jsmith@smith.com				
RECIPIENT: joe@mail.qa				
SUBJECT: Test message				
LAST STATE: N/A				
Displaying 1 — 3 of 3 items.				

- 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 \mathcal{T} and you specify that the subject begins with \mathcal{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, IronPort message ID (MID), and the names of any attachments. To view detailed information about a message, click the Show Details link for that message. For more information, see [Message Details, page 3-7](#).



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*
Message Tracking

Message Details	
Envelope and Header Summary	
Received Time:	14 Aug 2007 11:23:02 (GMT -0700)
MID:	10
Message Size:	1389 (Byte)
Subject:	Test1
Envelope Sender:	jsmith@smith.com
Envelope Recipients:	joe@mail.qa
Message ID Header:	000001c7dea0\$23f411c0\$d510fb0a@ironportsystems.com
IronPort Host:	elroy.run (172.19.0.11)
SMTP Auth User ID:	N/A
Sending Host Summary	
Reverse DNS Hostname:	None (unverified)
IP Address:	10.251.20.172
SBRS Score:	None
Processing Details	
	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: joe@mail.qa
14 Aug 2007 11:23:02 (GMT -0700)	Message 10 matched per-recipient policy DEFAULT for inbound mail policies.
14 Aug 2007 11:23:02 (GMT -0700)	Message 10 processed by Anti-Spam engine CASE. Verdict: definitely negative
14 Aug 2007 11:23:02 (GMT -0700)	Message 10 processed by Anti-Virus engine Sophos. Verdict: CLEAN
14 Aug 2007 11:23:02 (GMT -0700)	Virus scan verdict: negative for 10
14 Aug 2007 11:23:02 (GMT -0700)	Message 10 queued for delivery.
14 Aug 2007 11:23:02 (GMT -0700)	Message processing complete. (DCID 0) Message 10 to joe@mail.qa .unknown.
14 Aug 2007 11:23:02 (GMT -0700)	Message 10 to joe@mail.qa received remote SMTP response '/dev/null'.

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 Cisco 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.”

Attachments: The names of files attached to the message. For performance reasons, the names of files within attachments, such as OLE objects or archives such as .ZIP files, are not searched.

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.



CHAPTER 4

Quarantines

Quarantines are special queues or repositories used to hold and process messages. Cisco IronPort AsyncOS allows you to place incoming or outgoing messages into one of the appliance's 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, page 4-1](#)
- [Managing System Quarantines via the Graphical User Interface \(GUI\), page 4-3](#)
- [Working with Messages in System Quarantines, page 4-8](#)
- [Configuring the Cisco IronPort Spam Quarantines Feature, page 4-18](#)
- [Working with Safelists and Blocklists, page 4-37](#)

Quarantines Overview

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

Quarantine Types

A Cisco 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 Cisco IronPort Spam quarantine, stored on the Cisco IronPort appliance. You can also send messages to an external Cisco IronPort Spam quarantine, stored on a separate Cisco IronPort appliance. Cisco 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 Outbreak Filters.

System Quarantines

Typically, messages are placed in system quarantines due to a filter action. Additionally, the 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 4-3](#)) 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 Outbreak Filters feature - hold messages flagged by the Outbreak Filters feature until a anti-virus or anti-spam update is released. For more information about the Outbreak Filters feature, see the “Outbreak Filters” chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

Your Cisco 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 Outbreak Filters feature created when the 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 4-3](#).

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*).

Cisco IronPort Spam Quarantines

AsyncOS can be configured to send both spam and suspected spam to a Cisco 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 Cisco 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 4-24](#)).

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

For more information about Cisco IronPort Spam quarantines, see [Managing Messages in Cisco IronPort Spam Quarantines](#), page 4-35.

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

Quarantines				
Add Quarantine...				
Quarantine	Messages	Default Action	Status	Settings
Spam Quarantine (IP Interface not configured) **	0	Retain 14 days then Delete	<div><div></div></div> 0% Full	Edit
Outbreak [Manage by Rule Summary]	0	Retention Varies Action: Release	<div><div></div></div> 0% Full	Edit
Policy	0	Retain 10 days then Delete	<div><div></div></div> 0% Full	Edit
Virus	0	Retain 30 days then Delete	<div><div></div></div> 0% Full	Edit
** This Quarantine cannot be used until the Spam Quarantine HTTP or HTTPS service is enabled on one of your IP Interfaces. Go to Network > IP Interfaces to configure this.				

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 4-3). Also displayed is the status of the quarantine, including whether or not the associated security service (anti-virus scanning for the Virus quarantine, and 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 Cisco 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 Cisco IronPort Spam Quarantines Feature](#), page 4-18.

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 Cisco 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 4-3](#).

Table 4-1 Space Available for Quarantines on Cisco IronPort Appliances

Cisco IronPort Appliance	Storage Space	Outbreak Filters Storage Space*
X1050/1060/1070	10GB	3GB
C650/660/670	10GB	3GB
C350/360/370	4GB	2GB
C150/160	2.5GB	1GB

* Additional space when licensing the 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 4-4](#)) 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 is 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 4-6](#).

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).



Note

The retention time for messages in the Outbreak Filters quarantine are configured in the appliance's mail policies.

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 4-4](#)).

- 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 4-6](#). Messages released from quarantine because of a queue-full condition (early expiration) can optionally have other operations performed on them. For more information, see [When Allocated Space is Exceeded Send Messages and:, page 4-5](#).

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 4-16](#).

**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.

When Allocated Space is Exceeded Send Messages and:

The When Allocated Space is Exceeded Send Messages and: 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.

System Quarantine Performance

Messages stored in system quarantines use system memory in addition to hard drive space. Storing hundreds of thousands of messages in system quarantines on a single appliance may cause a decrease in the appliance's performance due to excessive memory usage. The appliance takes more time to quarantine, delete, and release messages, which causes message processing to slow down and the email pipeline to back up.

Cisco recommends storing an average of less than 20,000 messages in your system quarantines to ensure that Email Security appliance processes email at a normal rate.

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, as well as custom user roles with quarantines access privileges, 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. Users in the Technicians group cannot access quarantines.

Creating System Quarantines

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

1. Create users who will interact with the quarantine.
 - a. **Local 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 [Working with User Accounts, page 8-12](#).
 - b. **External Users.** You can also enable your Cisco 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 8-23](#).
 - c. **Delegated Administrators.** You can create a custom user role with quarantine access privileges and assign local users to the group to act as delegated administrators for the quarantine. For more information, see [Managing Custom User Roles for Delegated Administration, page 8-26](#).
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 4-4 . |
| Step 4 | Select a Retention Period, or time to keep a message in the quarantine before the default action is performed on the message. For more information, see Retention Time, page 4-4 . |
| 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 4-5](#).
- Step 7** If you want to add an X-Header, enter the name and value. For more information, see [Add X-Header, page 4-5](#).
- 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 4-5](#).
- Step 9** Select users to access this quarantine by clicking on Local Users link and select the check boxes for the users you want to access the quarantine. A quarantine's user list contains local users in all user groups, except Administrators and Technicians. Users in the Administrators group always have full access to the quarantine and users in the Technicians group cannot access quarantines. For more information, see [Users and User Groups, page 4-6](#). The link is not available if you have not yet created any users.
- Step 10** Optionally, check the link for Externally Authenticated Users and select the check boxes for the user roles of externally authenticated users to access the quarantine. Externally authenticated users are authenticated by your Cisco IronPort appliance using a centralized authentication system. For more information, see [External Authentication, page 8-23](#).
- Step 11** Optionally, click the link for Custom User Roles if you want delegated administrators to access the quarantine. Select the check boxes for the custom user roles with quarantine access privileges and click OK. For more information, see [Managing Custom User Roles for Delegated Administration, page 8-26](#).
- Step 12** 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*
Edit Policy Quarantine

Settings		Delete Quarantine
Quarantine Name:	Policy	
Space Allocation:	1024 MB (Maximum Size 3072 MB)	
Default Action:	Retain 10 Days then Delete	
When Allocated Space is Exceeded Send Messages and:	Modify Subject:	None
	Add X-Header:	Name: Value:
	Strip Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Local Users:	brad1	
Externally Authenticated Users:	External authentication is disabled. Go to System Administration > Users to enable external authentication.	
Custom User Roles:	Policy Administrator, Quarantine Manager	
Cancel		Submit

- 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

The screenshot shows the 'Edit Policy Quarantine' settings page. At the top right, there is a red box around the 'Delete Quarantine' link. The settings include: Quarantine Name: Policy; Space Allocation: 1024 MB (Maximum Size 3072 MB); Default Action: Retain 10 Days then Delete; When Allocated Space is Exceeded Send Messages and: Modify Subject: None; Add X-Header: Name: , Value: ; Strip Attachments: No; Local Users: No users selected; Externally Authenticated Users: External authentication is disabled. Go to System Administration > Users to enable external authentication; Custom User Roles: Policy Administrator, Quarantine Manager. At the bottom are 'Cancel' and 'Submit' buttons.

- Step 2** A confirmation message is displayed:

Figure 4-4 *Confirming a System Quarantine Deletion*

The screenshot shows a 'Confirm Delete' dialog box with the text 'Are you sure you want to delete "Policy"?'. There are 'Cancel' and 'Delete' buttons at the bottom.

- 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

Quarantines				
Add Quarantine...				
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 Policy Quarantine

Messages						
Search Query: All messages			View All Messages		Search Quarantine...	
<input type="checkbox"/>	To	From	Subject	Received	Scheduled Exit	In other quarantine
<input type="checkbox"/>	randchrist@saint...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	polynesiancr@set...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	anabelle_ng@bigf...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	earlene.taylor-2...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	lingwu@aol.com.exa...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	bks4q@virginia.e...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	uglytom@uglytown...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
<input type="checkbox"/>	lucybeane1@aol.c...	user123@example.cc	Testing	11 May 08:21 (GMT -07)	21 May 08:21 (GMT -07)	1K
Select Action... Submit						

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 4-15](#) 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 Outbreak Filters Feature and the Outbreak Quarantine](#), page 4-17.

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				
<input type="checkbox"/> All	<input type="checkbox"/> Quarantine	<input type="checkbox"/> Reason	<input type="text" value="Time Received"/>	<input type="text" value="Time Scheduled to Exit"/>
<input type="checkbox"/> 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:		<input type="button" value="Start Test"/>		
Send Copy To:		E-Mail Addresses, comma separated: <input type="text"/> <input type="button" value="Send"/>		
Envelope Sender:		user@test.com		
Recipients:		user1@test.com		
Subject:		DLPTEST		
Matched Content				
<input type="checkbox"/> Policy				
Attachment Name	Matched Content	Condition		
FP1.1.txt	<ul style="list-style-type: none"> 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				
<pre>X-IronPort-AV: E=Sophos;i=4.43,282,1246818600; d="txt?scan?208";a="178202" Received: from d2.vmw023-bad04.iqaa (HELO vmw023-bad04.iqaa) ([172.22.107.1]) by c360q02.iqaa with ESMTP; 28 Jul 2009 16:25:03 +0530 Message-ID: <792087.518002035-sendEmail@vmw023-bad04> 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"</pre>				
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 Outbreak Filters Feature and the Outbreak Quarantine, page 4-17](#) 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

Attachment Name	Matched Content	Condition
FF1.3.txt	<ul style="list-style-type: none"> MS 38930 USA Facilities 662-646-0523 jsmuelson@acmecorp.com 7/17/06 4526132070312710 Acme Corp Intra Globe 808 Summer Street Greenwood MS 38930 USA Publishing 662-646-0722 iglobe@acmecorp.com 2/1/07 446213193071560 Acme Corp X-mthry License 808 Summer Street Greenwood MS 38930 USA Marketing 662-646-0541 klape@acmecorp.com 2/1/07 471420862521010 Acme Corp Marty Smith 808 Summer Street Greenwood MS 38930 USA Fontenawinn 662-646-0543 	DLP Classifier: Content Information

Header

X-ProofKey-Ali: E="topher.w@4.43.202.1246888600", d="text/plain; charset=UTF-8"

Received: from d2.vmm023-bad04.bpe (HELO vmm023-bad04.bpe) ([172.22.107.1]) by c360402-bpe with ESMTP; 28 Jul 2009 16:25:03 +0530

Message-ID: <792007.518002035-sendEmail@vmm023-bad04>

From: "user@test.com" <user@test.com>

To: "user1@test.com" <user1@test.com>

Subject: DUPEST

Date: Tue, 28 Jul 2009 09:42:11 +0000

X-Mailer: sendEmail 1.50

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="-----MIME delimiter for sendEmail-538925-714612664"

Message

Test

Message Parts

Name	Size	Details
[message body]	6	ASCII text, with CRLF line terminators
FF1.3.txt	1K	ASCII text

Selecting a Message Action

The three possible actions are to delete the message, release it, or delay the expiration. See [Default Action](#), page 4-4 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 4-15 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 <input type="button" value="v"/>
For Messages Received:	Last day <input type="button" value="v"/>
Envelope Sender:	Contains <input type="button" value="v"/> <input type="text"/>
Envelope Recipient(s):	Contains <input type="button" value="v"/> <input type="text"/>
Subject:	Contains <input type="button" value="v"/> <input type="text"/>
Display:	20 <input type="button" value="v"/> Per page

- 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 4-9](#) for more information.

Multi-User Access and System Quarantines

AsyncOS supports delegation of quarantine management by allowing you to specify users from the Operators, Help Desk Users, and Guests groups, as well as users from custom user roles with quarantine access privileges, 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

These 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 and user roles, see the [Working with User Accounts, page 8-12](#) and [Managing Custom User Roles for Delegated Administration, page 8-26](#).

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:

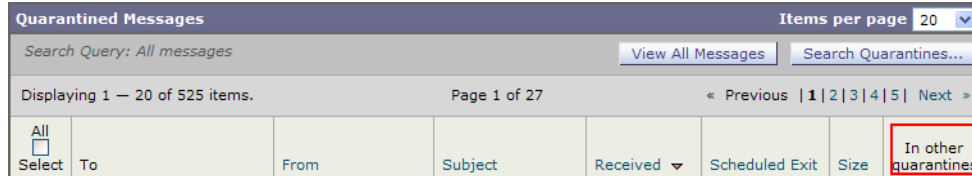
- A message is not released from any quarantine until it has been released from all of the quarantines in which it resides.
- If a message is marked as Deleted in any quarantine, it is not deliverable from any other quarantine in which it resides. It can still be released, but it will not be delivered.

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 it has been quarantined, it will be rescanned for viruses and spam (assuming anti-virus and spam are enabled on that mail policy) before it can be delivered.

When a message is released from quarantine it is scanned for viruses and spam by the anti-virus and anti-spam engines (if anti-virus is enabled). If the verdict produced 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 another 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 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 Outbreak Filters Feature and the Outbreak Quarantine

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

If the license for the 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 Cisco IronPort feature when viewing message details, and the option to sort messages in sort results by Scheduled Exit time.

If anti-spam and anti-virus are enabled on the appliance, the scanning engines scan 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 “Outbreak Filters” chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.


Send to Cisco IronPort Systems

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

To send a copy of a message to Cisco IronPort:

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

Figure 4-12 Searching Quarantines



The screenshot shows a web interface for message details. Under the 'Test for Viruses' section, there is a 'Start Test' button. Below that, in the 'Send Copy To' section, there are two checkboxes: 'E-Mail Address:' followed by a text input field, and 'Send a Copy to IronPort Systems'. The 'Send a Copy to IronPort Systems' checkbox is highlighted with a red rectangular box. To the right of these checkboxes is a 'Send' button.

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

Configuring the Cisco IronPort Spam Quarantines Feature

Each Cisco IronPort appliance can have a local Cisco IronPort Spam quarantine enabled if the Cisco IronPort anti-spam has been enabled. Each Cisco IronPort appliance can also refer to an external Cisco IronPort Spam quarantine, configured on another Cisco IronPort appliance (typically an M-Series appliance, see “The Cisco 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 Cisco IronPort Spam quarantine is enabled the *local* Cisco IronPort Spam quarantine is used.

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

- Step 1** Add an external Cisco IronPort Spam quarantine (see [Configuring an External Cisco IronPort Spam Quarantine, page 4-27](#)) or enable and configure the local Cisco IronPort Spam quarantine (see [Configuring the Local Cisco IronPort Spam Quarantine, page 4-22](#)). Configuring the local Cisco 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 Cisco IronPort Spam quarantine, edit an IP interface and enable the Cisco IronPort Spam quarantine HTTP or HTTPS service (see [Enabling the Cisco IronPort Spam Quarantine HTTP/S Service on an IP Interface, page 4-28](#)). Enabling the Cisco IronPort Spam quarantine HTTP/S service allows you to access the quarantine.
- Step 3** If you want to migrate from a local Cisco IronPort Spam quarantine to an external Cisco 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 Cisco IronPort Spam Quarantine to an External Quarantine, page 4-20](#)).
- Step 4** Configure the anti-spam scanning options for the policy to send spam or suspect spam (or both) to the Cisco IronPort Spam Quarantine (see [Enabling Cisco IronPort Spam Quarantines for a Mail Policy, page 4-29](#)). This step is where you actually configure the system to quarantine spam or suspect spam.
- Step 5** See [Considerations for Deployment, page 4-30](#). This important section provides a wealth of additional guidance and information about the Cisco IronPort Spam quarantine, including notifications, authentication, and configuration of other related AsyncOS features.

Enabling and Disabling the Local Cisco IronPort Spam Quarantine

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

To enable the local Cisco IronPort Spam quarantine:

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

Figure 4-13 Enabling the Local Cisco IronPort Spam Quarantine Quarantines

Quarantines				
Add Quarantine...				
Quarantine	Messages	Default Action	Status	Settings
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 Cisco IronPort Spam Quarantine is enabled. If the Cisco IronPort Spam Quarantine is not configured, the Edit IronPort Spam Quarantine page is displayed (see [Configuring the Local Cisco IronPort Spam Quarantine, page 4-22](#)).
- Step 3** Submit and commit your changes.

Disabling the Local Cisco IronPort Spam Quarantine

To disable the local Cisco 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 Cisco 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 Cisco 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				
Add Quarantine...				
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	<input type="text"/> 0% Full	Edit
Policy	0	Retain 10d then Delete	<input type="text"/> 0% Full	Edit
Virus	0	Retain 30d then Delete	<input type="text"/> 0% Full	Edit



Note

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

Disabled Cisco IronPort Spam Quarantines and Mail Policies

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

Migrating from a Local Cisco IronPort Spam Quarantine to an External Quarantine

If you are currently using the local Cisco IronPort Spam Quarantine on a local Cisco IronPort C- or X-Series appliance but would like to migrate to an external Cisco IronPort Spam Quarantine hosted on an Cisco 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 then click the “Delete All” link on the local quarantines page (see [Deleting Messages from the Cisco IronPort Spam Quarantine, page 4-37](#)). This link only becomes available when a local Cisco 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.

Cisco IronPort Spam Quarantine Settings

Spam Quarantine Settings

Set quarantine size, deletion/retention policy, default language, and enable or disable Cisco IronPort notification. By default the local Cisco 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 Cisco IronPort Spam quarantine, including specifying a custom logo and login page message. See [Configuring Spam Quarantine Settings for the Local Cisco IronPort Spam Quarantine](#), page 4-22.

Specify AsyncOS Operator users that may view or interact with the messages in the local Cisco IronPort Spam quarantine. All Administrator level users (such as the default ‘admin’ user) created in AsyncOS are automatically able to access and modify the Cisco IronPort Spam quarantine. Operators can view quarantine contents, but may not change the quarantine settings. See [Configuring Administrative Users for Cisco IronPort Spam Quarantines](#), page 4-23.

Cisco IronPort Spam Quarantine Access

Allow end users to access and manage their messages in the Cisco 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 4-24. Specifying “None” indicates that end users will only be allowed to access the Cisco 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
<i>Disabled</i>	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 Cisco 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 Cisco 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 4-33). See [Configuring Spam Notifications](#), page 4-25.

**Note**

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

Configuring the Local Cisco IronPort Spam Quarantine

Once the local Cisco IronPort Spam quarantine is enabled (see [Enabling and Disabling the Local Cisco IronPort Spam Quarantine, page 4-19](#)), you can edit the quarantine’s settings to configure the Cisco IronPort Spam quarantine and how users will interact with it.

To configure the local Cisco 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 Cisco IronPort Spam Quarantine

To edit the Cisco IronPort Spam Quarantine settings for the Cisco IronPort Spam quarantine on the local Cisco 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*
Edit Spam Quarantine

Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable Spam Quarantine	
Quarantine Size:	Total: <input type="text" value="2.5"/> <input type="text" value="GB"/> (15.0 GB maximum)
<input checked="" type="checkbox"/> When storage space is full, automatically delete oldest messages first	
Schedule Delete After:	<input checked="" type="radio"/> 14 days <input type="radio"/> Do not schedule delete
Notify IronPort Upon Message Release:	<input type="checkbox"/> Send a copy of released messages to IronPort for analysis(recommended)
Spam Quarantine Appearance:	<div> Current Logo: </div> <div> <input checked="" type="radio"/> Use Current Logo <input type="radio"/> Use IronPort Spam Quarantine Logo <input type="radio"/> Upload Custom Logo: <input type="text"/> <input type="button" value="Browse..."/> <small>Maximum size 500w x 50h pixels</small> </div> <div> Login Page Message: <input type="text"/> </div>
Administrative Users: ?	<div>Local Users: No users selected</div> <div>Externally Authenticated Users: External authentication is disabled. Go to System Administration > Users to enable external authentication.</div> <div>Custom User Roles: No user roles selected</div>

- 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. Cisco 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. Cisco 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 Cisco IronPort for analysis. Cisco 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 Cisco IronPort Spam Quarantine logo is used.



Note If you specify a custom logo the Cisco 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 Cisco IronPort M-Series appliance, see the *Cisco IronPort AsyncOS for Security Management User Guide* for more information.

Configuring Administrative Users for Cisco IronPort Spam Quarantines

You can specify administrative users for the Cisco IronPort Spam quarantine. In this case, “administrative” refers to the user’s access to the Cisco IronPort Spam quarantine. Operators, help desk users, read-only operators, and delegated administrators belonging to custom user roles with quarantine privileges 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 Cisco 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 Cisco IronPort Spam quarantine:

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

Administrative Users: ?	Local Users: brad1
Externally Authenticated Users:	<i>External authentication is disabled. Go to System Administration > Users to enable external authentication.</i>
Custom User Roles:	Quarantine Manager

- Step 1** Click on the link for the appropriate type of user: local, externally authenticated, or custom role (delegated administrators).
- Step 2** Select the users you want to add.
- Step 3** Click **Add**.
- Note that Operator level users and delegated administrators may view messages in the Cisco IronPort Spam quarantine, but may not edit the settings of the quarantine. Administrative users can view messages and change the settings.
- Step 4** Submit and commit your changes.

Configuring End User Quarantine Access

To allow end users to access the Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco 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 4-24](#)). 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 Cisco 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 Cisco IronPort appliance, then multiple recipients may have access to the same quarantine for that list.

Because of the way the Cisco 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 4-30](#) and [Receiving Multiple Notifications, page 4-33](#) 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*

Spam Notifications

☒ Enable Spam Notification

From Address: "friendly name" (optional) <username@hostname>
(example: "Email Administrator" <notify@company.com>)

Subject: IronPort Spam Quarantine Notification

Title: IronPort Spam Quarantine Notification

Message Body: ?
The message(s) below have been blocked by your administrator as suspected spam.
There are %new_message_count% new messages in your Email Quarantine since you received your last IronPort Quarantine Notification. If the messages below are spam, you do not need to take any action. Messages will be automatically removed from the quarantine after %days_until_expire% day(s).
If any of the messages below are not spam, click the Release link to have them sent to your Inbox. To see all quarantined messages view %quarantine_url%.
Preview Message

Message Variables

- New Message Count
- Total Message Count
- ..
- Days Until Message Expires
- Quarantine URL
- Username
- New Message Table

Message Format: HTML (recommended)

Deliver Bounce Message To: (e.g. mybounceaddress@company.com)

Consolidate Notifications: ☐ Consolidate notifications sent to the same LDAP user at different addresses
This setting uses the LDAP Alias Consolidation Query configured at System Administration > LDAP.

Notification Schedule: ☐ Monthly (Sent the 1st of each month at 12am)
☒ Weekly Monday (Sent at 12am)
☐ Daily (weekdays) %
12 3 6 9 AM
12 3 6 9 PM

- 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 4-30).
- 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 Cisco IronPort Spam Quarantine

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

If you use an external Cisco IronPort Spam quarantine, the quarantine settings are configured on that Cisco IronPort appliance. If you have both the local and an external Cisco IronPort Spam quarantine enabled on your Cisco IronPort appliance, the local Cisco 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 Cisco IronPort Spam Quarantine

To add an external Cisco 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



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 Cisco IronPort Spam Quarantine

To edit an existing external Cisco 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 Cisco IronPort Spam Quarantine

You can only have one external Cisco IronPort Spam quarantine specified on your Cisco IronPort appliance. Please note that removing an external Cisco 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 Cisco IronPort Spam quarantine is removed from the local machine.

To remove an external Cisco 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

External Quarantine Settings	
Type:	IronPort Anti-Spam
Name:	spam_quarantine (e.g. spam_quarantine)
IP Address:	1.2.3.4
Port:	5025

Cancel Submit

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

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

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

To enable the Cisco 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
Edit IP Interface

IP Interface Settings																											
Name:	Management																										
Ethernet Port:	Management																										
IP Address:	172.19.0.11 *																										
Netmask:	255.255.255.0 *																										
Hostname:	elroy.run																										
Services:	<table border="1"> <thead> <tr> <th>Service</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> FTP</td> <td>21</td> </tr> <tr> <td><input checked="" type="checkbox"/> Telnet</td> <td>23</td> </tr> <tr> <td><input checked="" type="checkbox"/> SSH</td> <td>22 *</td> </tr> <tr> <td colspan="2">Appliance Management</td> </tr> <tr> <td><input checked="" type="checkbox"/> HTTP</td> <td>80 *</td> </tr> <tr> <td><input checked="" type="checkbox"/> HTTPS</td> <td>443 *</td> </tr> <tr> <td colspan="2"><input checked="" type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)</td> </tr> <tr> <td colspan="2">IronPort Spam Quarantine</td> </tr> <tr> <td><input checked="" type="checkbox"/> HTTP</td> <td>82</td> </tr> <tr> <td><input checked="" type="checkbox"/> HTTPS</td> <td>83</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)</td> </tr> <tr> <td colspan="2"> <input checked="" type="checkbox"/> This is the default interface for IronPort Spam Quarantine Quarantine login and notifications will originate on this interface. URL Displayed in Notifications: <input checked="" type="radio"/> Hostname <input type="radio"/> (examples: http://spamQ.url, http://10.1.1.1:82/) </td> </tr> </tbody> </table>	Service	Port	<input type="checkbox"/> FTP	21	<input checked="" type="checkbox"/> Telnet	23	<input checked="" type="checkbox"/> SSH	22 *	Appliance Management		<input checked="" type="checkbox"/> HTTP	80 *	<input checked="" type="checkbox"/> HTTPS	443 *	<input checked="" type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)		IronPort Spam Quarantine		<input checked="" type="checkbox"/> HTTP	82	<input checked="" type="checkbox"/> HTTPS	83	<input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)		<input checked="" type="checkbox"/> This is the default interface for IronPort Spam Quarantine Quarantine login and notifications will originate on this interface. URL Displayed in Notifications: <input checked="" type="radio"/> Hostname <input type="radio"/> (examples: http://spamQ.url, http://10.1.1.1:82/)	
Service	Port																										
<input type="checkbox"/> FTP	21																										
<input checked="" type="checkbox"/> Telnet	23																										
<input checked="" type="checkbox"/> SSH	22 *																										
Appliance Management																											
<input checked="" type="checkbox"/> HTTP	80 *																										
<input checked="" type="checkbox"/> HTTPS	443 *																										
<input checked="" type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)																											
IronPort Spam Quarantine																											
<input checked="" type="checkbox"/> HTTP	82																										
<input checked="" type="checkbox"/> HTTPS	83																										
<input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)																											
<input checked="" type="checkbox"/> This is the default interface for IronPort Spam Quarantine Quarantine login and notifications will originate on this interface. URL Displayed in Notifications: <input checked="" type="radio"/> Hostname <input type="radio"/> (examples: http://spamQ.url, http://10.1.1.1:82/)																											

* Warning - Please exercise care when disabling or changing these items, as this could disrupt active connections to this appliance when changes to these items are committed.

Cancel

Submit

- 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 Cisco 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 Cisco IronPort Spam Quarantines for a Mail Policy

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

To configure a mail policy to send spam or suspect spam to the Cisco 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 Incoming Mail Policies*

Find Policies

Email Address: Recipient ☒ Sender ☐ Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	scan_for_confidential ex_employee	Retention Time: Virus: 1 day Other: 4 hours	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Deliver Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	scan_for_confidential no_mp3s ex_employee	Retention Time: Virus: 1 day	

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 Mail Policies: Anti-Spam*

Anti-Spam Settings

Policy: Default

Enable Anti-Spam Scanning for This Policy: ☒ Use IronPort Anti-Spam service ☐ Disabled

Positively-Identified Spam Settings

Apply This Action to Message: Drop

Add Text to Subject: Deliver Drop Spam Quarantine Bounce custom header and message delivery.

Advanced

Suspected Spam Settings

Enable Suspected Spam Scanning: ☐ No ☒ Yes

Apply This Action to Message: Deliver

Send to Alternate Host (optional):

Add Text to Subject: Prepend [(SUSPECTED SPAM)]

Advanced Optional settings for custom header and message delivery.

Marketing Email Settings

Enable Marketing Email Scanning: ☒ No ☐ Yes

Apply This Action to Message: Deliver

Send to Alternate Host (optional):

Add Text to Subject: Prepend [(MARKETING)]

Advanced Optional settings for custom header and message delivery.

Spam Thresholds

Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.

IronPort Anti-Spam: ☐ Use the Default Thresholds ☒ Use Custom Settings:

Positively Identified Spam: Score > (50 - 100)

Suspected Spam: Score > (minimum 25, cannot exceed positive spam score)

Cancel Submit

Step 4 Repeat this for Suspected spam and Marketing email 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 Cisco IronPort Spam quarantine.

Disk Space

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

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

Model	Disk Space (in GBytes)
C150/160	5
C350/360/370	15
C650/660/670	30
X1050/1060/1070	30

End Users Accessing the Cisco IronPort Spam Quarantine

End users can access the Cisco 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 4-24).

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 Cisco 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 Cisco IronPort Spam quarantine can bind as in order to execute the search.
 - Step 3** The Cisco IronPort Spam quarantine then searches for the user using the specified BaseDN and Query String. When a user’s LDAP record is found, the Cisco 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 Cisco IronPort Spam quarantine still needs to determine which mailboxes’ contents to show for that user.
 - Step 4** Messages are stored in the Cisco IronPort Spam quarantine using the recipient's envelope address. After a user's password is validated against LDAP, the Cisco 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 4-24).
- Step 2** The Cisco 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 Cisco IronPort Spam quarantine immediately logs out of the IMAP/POP server.
- Step 3** Once the user is authenticated, the Cisco IronPort Spam Quarantine lists email for the user, based on the email address:
- If you have configured the Cisco 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 Cisco IronPort Spam quarantine uses the entered email address to search for matching envelopes.

Determining the URL for Logging in to the Cisco IronPort Spam Quarantine

The URL end users can use to access the Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco IronPort Spam Quarantine, page 4-31](#).

Keep in mind that email addresses are case insensitive in the Cisco 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 Cisco 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 Cisco IronPort appliance to specify a default encoding. Doing so will help ensure that these types of messages display properly in the Cisco 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 Cisco IronPort Spam Quarantines

This section explains how to work with messages within local or external Cisco 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 Cisco IronPort Spam quarantine:

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

Figure 4-24 IronPort Spam Quarantine Search Page

Searching for Messages in the Cisco IronPort Spam Quarantine

Use the search form to search through all of the messages in the Cisco 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 Cisco 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 Cisco IronPort appliance.

Viewing Messages in the Cisco IronPort Spam Quarantine

The message listing shows messages in the Cisco 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 Cisco 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 Cisco 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 Cisco IronPort Spam Quarantine

The Cisco IronPort Spam quarantine can be configured to automatically delete messages after a certain amount of time. Also, the Cisco 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 Cisco 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 Cisco IronPort Spam quarantine, disable the quarantine (see [Disabling the Local Cisco IronPort Spam Quarantine, page 4-19](#)) 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 Cisco 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 Cisco IronPort Spam Quarantine, so you *must* enable and configure the Cisco 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 Cisco 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 Cisco 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 Cisco 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 4-40](#).

For information about working with the backup .CSV database, see [Backing Up and Restoring the Safelist/Blocklist Database, page 4-40](#).

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 Cisco 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 4-39](#).
- **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 Cisco 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 4-41](#).

Message Delivery For Safelists and Blocklists

When you enable safelists and blocklists, the Cisco IronPort appliance scans the messages against the safelist/blocklist database immediately prior to anti-spam scanning. If the Cisco 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 Cisco 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 Cisco IronPort Spam Quarantine.** Because the safelist and blocklist is accessed from the Cisco IronPort Spam Quarantine, you must enable this feature to use safelists and blocklists. For information, see [Configuring the Cisco IronPort Spam Quarantines Feature](#), page 4-18.
- **Enable and configure the Safelist/Blocklist feature.** Once the Cisco 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 4-39
- **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 4-40.
- **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 Cisco 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 4-40.
- **Troubleshooting Safelists and Blocklists.** To troubleshoot safelists and blocklists, you can check logs, alerts. For more information, see [Troubleshooting Safelists and Blocklists](#), page 4-41.

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 Cisco 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**.

Figure 4-26 End-User Safelist/Blocklist 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 Cisco IronPort appliance saves the database as a .CSV file. The .CSV file is maintained separately from the XML configuration file that contains your Cisco IronPort appliance configuration settings. If you upgrade your Cisco 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 Cisco IronPort appliance saves a .CSV file to the `/configuration` directory using the following naming convention:

`slbl<timestamp><serial number>.csv`

You can do the backup and restore from either the System Administration > Configuration File page in the GUI or the `slblconfig` command in the CLI.

From the CLI, use the `slblconfig -> export` command to back up the database to the `/configuration` directory. Use the `slblconfig -> import` command to restore the database from a backup. Choose the database you want to use from a list of backup files in the `/configuration` directory. You can choose whether to ignore invalid entries.

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.

Figure 4-27 End-User Safelist/Blocklist Database

- Step 2** To back up a database to a .CSV file, click **Backup Now**.

- Step 3** To restore the database, click **Select File to Restore**.

The Cisco 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 Cisco 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 Cisco 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
C150/C160	10 minutes
C350/C360/C370	15 minutes

Table 4-5 Synchronization for Safelist and Blocklist Settings

Appliance	Synchronization Time
C650/C660/C670	30 minutes
X1050/X1060/X1070	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 Cisco 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 Cisco 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 Cisco IronPort Spam Quarantine accounts. For more information, see [Accessing Safelists and Blocklists, page 4-42](#).
- **Add safelist entries.** Users add safelist entries from the Options menu or the list of quarantined messages in Cisco IronPort Spam Quarantine. For more information, see [Adding Entries to Safelists, page 4-42](#).
- **Add blocklist entries.** Users add blocklist entries from the Options menu of the Cisco IronPort Spam Quarantine. For more information, see [Adding Entries to Blocklists, page 4-44](#).

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 Cisco 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 Cisco 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 Cisco IronPort appliance delivers all mail from *example.com* without scanning for spam, but will treat mail from *george@example.com* as spam.

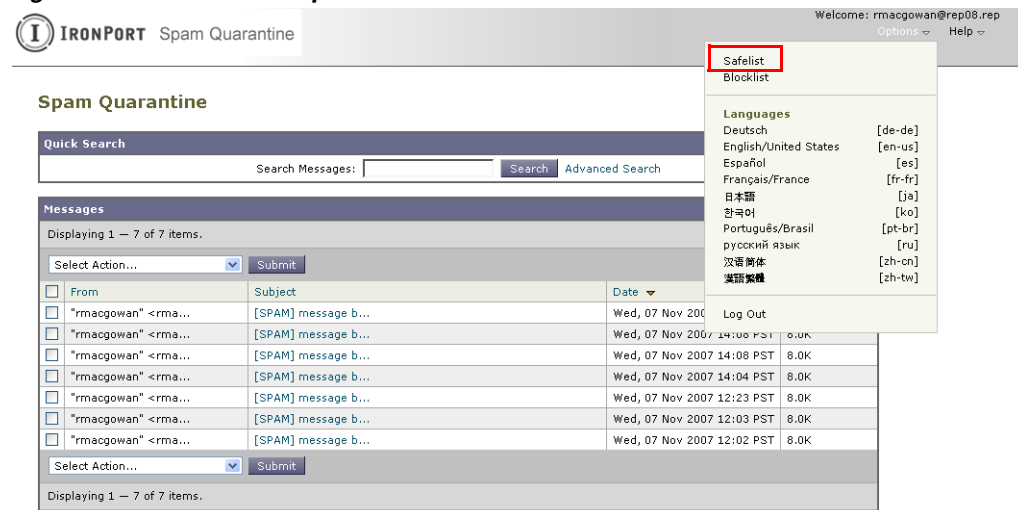
End users cannot allow or block a range of sub-domains using the following syntax: *.domain.com*. However, an end user can explicitly block a specific domain using the following syntax: *server.domain.com*.

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 4-28 Safelist Options in the End-User Quarantine

Copyright © 2003-2007 IronPort Systems, Inc. All rights reserved.

- 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 4-29 Safelist in End-User Quarantine

Success — The sender `laura@yahoo.com` has been added to the Safelist.

Email addresses or domains added to this list will not be identified as Spam.

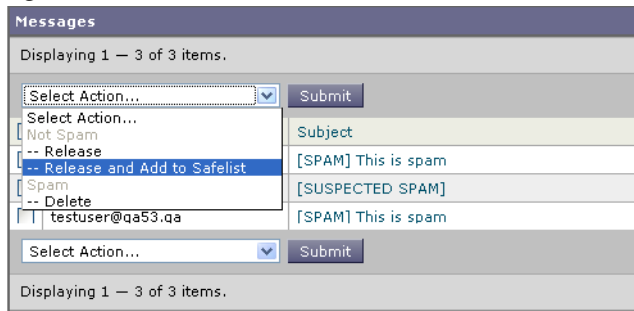


[View Spam Quarantine](#)

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.

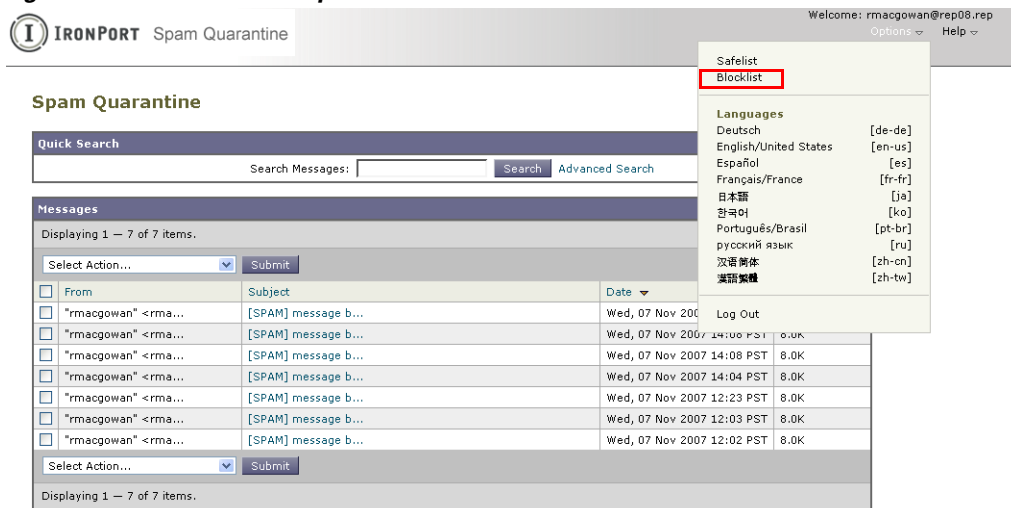
Figure 4-30 Safelist in End-User Quarantine

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 4-31 Blocklist Options in the End-User Quarantine

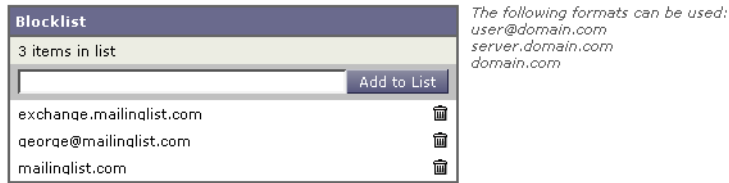
Copyright © 2003-2007 IronPort Systems, Inc. All rights reserved.

- 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 4-32 Adding Senders to a Blocklist

Success — The sender george@mailinglist.com has been added to the Blocklist.

Email addresses or domains added to this list will always be identified as Spam.



[View Spam Quarantine](#)

When the Cisco 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/blocklist action settings.

**Note**

Unlike safelist entries, you can only add blocklist entries from the Options menu in the End-User Quarantine.



CHAPTER 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, page 5-1](#)
- [Log Types, page 5-7](#)
- [Log Subscriptions, page 5-38](#)

Overview

This section contains the following topics:

- [Understanding Log Files and Log Subscriptions, page 5-1](#)
- [Log Types, page 5-2](#)
- [Log Retrieval Methods, page 5-6](#)

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 Cisco 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.

Cisco offers an off-box centralized reporting and tracking tool for logs from multiple Cisco IronPort appliances. See your Cisco 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.

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 5-38 for more information.

Cisco 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.
Delivery Logs	Delivery logs record critical information about the email delivery operations of the Cisco 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 <code>status detail</code> and <code>dnsstatus</code> . The period of recording is set using the <code>setup</code> subcommand in <code>logconfig</code> . 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.
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 <code>commit</code> command. System logs are useful for troubleshooting the basic state of the appliance.

Table 5-1 Log Types (continued)

Log	Description
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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> .
LDAP Debug Logs	LDAP debug logs are meant for debugging LDAP installations. (See the “LDAP Queries” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i> .) Useful information about the queries that the Cisco IronPort appliance is sending to the LDAP server are recorded here.
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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> .
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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> .
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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>). 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 Cisco IronPort Spam Quarantine processes.
IronPort Spam Quarantine GUI Logs	IronPort Spam Quarantine logs record actions associated with the Cisco 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.

Table 5-1 Log Types (continued)

Log	Description
Safe/Block Lists Logs	Safelist/blocklist logs record data about the safelist/blocklist settings and database.
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.
Configuration History Logs	Configuration history logs record the following information: What changes were made on the Email Security appliance, and when were the changes made? A new configuration history log is created each time a user commits a change.

Log Type Characteristics

Table 5-2 summarizes the different characteristics of each log type.

Table 5-2 Log Type Comparison

						Contains								
	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	Configuration Information
IronPort Mail Logs	•		•			•	•	•	•	•		•		
qmail Format Delivery Logs		•			•		•	•	•			•		
Delivery Log		•			•		•	•	•			•		
Bounce Logs	•		•						•	•		•		
Status Logs		•	•			•								
Domain Debug Logs	•		•					•	•	•			•	

Table 5-2 Log Type Comparison (continued)

	Contains													
	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	Configuration Information
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				•										
Scanning Logs	•		•			•								•
IronPort Spam Quarantine	•		•			•								
IronPort Spam Quarantine GUI	•		•			•								
Safe/Block Lists Logs	•		•			•								
Reporting Logs	•		•		•									
Reporting Query Logs	•		•		•									
Updater Logs			•											
Tracking Logs	•				•	•	•	•	•	•		•		
Authentication Logs	•		•											
Configuration History 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*

Manually Download	<p>This method lets you access log files at any time by clicking a link to the log directory on the Log Subscriptions page, then clicking the log file to access. Depending on your browser, you can view the file in a browser window, or open or save it as a text file. This method uses the HTTP(S) protocol and is the default retrieval method.</p> <p>Note Using this method, you cannot retrieve logs for any computer in a cluster, regardless of level (machine, group, or cluster), even if you specify this method in the CLI.</p>
FTP Push	<p>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 8-40.</p>
SCP Push	<p>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.</p>
Syslog Push	<p>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.</p>

Log Filenames and Directory Structure

Cisco 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 `.current` or `.s` (signifying saved). You should only transfer or delete log files with the saved status.

Log Rollover and Transfer Schedule

Log files are created by log subscriptions, and are rolled over (and transferred, if a push-based retrieval option is selected) based on the first user-specified condition reached: maximum file size or scheduled rollover. Use the `logconfig` command in the CLI or the Log Subscriptions page in the GUI to configure both the maximum file size and time interval for scheduled rollovers. You can also use the **Rollover Now** button in the GUI or the `rollovernow` command in the CLI to rollover selected log subscriptions. See [Rolling Over Log Subscriptions, page 5-44](#) for more information on scheduling rollovers.

Logs retrieved using manual download are saved until they reach the maximum number you specify (the default is 10 files) or until the system needs more space for log files.

Logs Enabled by Default

Your Cisco 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). By default, the retrieval method is “Manually Download.”

Table 5-4 Pre-configured Log Subscriptions

Log #	Log Subscription Name	Log Type
1	antispam	Anti-Spam logs
2	antivirus	Anti-Virus Logs
3	asarchive	Anti-Spam Archive
4	authentication	Authentication Logs
5	avarchive	Anti-Virus Archive
6	bounces	Bounce Logs
7	cli_logs	CLI Audit Logs
8	encryption	Encryption
9	error_logs	IronPort Text Mail Logs
10	euq_logs	IronPort Spam Quarantine Logs
11	euqgui_logs	IronPort Spam Quarantine GUI Logs
12	ftpd_logs	FTP Server Logs
13	gui_logs	HTTP Logs
14	mail_logs	IronPort Text Mail Logs
15	reportd_logs	Reporting Logs
16	reportingqueryd_logs	Reporting Query Logs
17	scanning	Scanning Logs
18	slbld_logs	Safe/Block Lists Logs
19	sntpd_logs	NTP logs
20	status	Status Logs
21	system_logs	System Logs
22	trackerd_logs	Tracking Logs
23	updater_logs	Updater Logs

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 5-39](#) for more information. For information about creating new log subscriptions, or modifying existing ones, see [Log Subscriptions, page 5-38](#).

Log Types

This section covers the following topics:

- [Using IronPort Text Mail Logs, page 5-8](#)
- [Using IronPort Delivery Logs, page 5-15](#)

- [Using IronPort Bounce Logs, page 5-17](#)
- [Using IronPort Status Logs, page 5-19](#)
- [Using IronPort Domain Debug Logs, page 5-22](#)
- [Using IronPort Injection Debug Logs, page 5-23](#)
- [Using IronPort System Logs, page 5-24](#)
- [Using IronPort CLI Audit Logs, page 5-25](#)
- [Using IronPort FTP Server Logs, page 5-26](#)
- [Using IronPort HTTP Logs, page 5-27](#)
- [Using IronPort NTP Logs, page 5-28](#)
- [Using Scanning Logs, page 5-28](#)
- [Using IronPort Anti-Spam Logs, page 5-29](#)
- [Using IronPort Anti-Virus Logs, page 5-29](#)
- [Using IronPort Spam Quarantine Logs, page 5-30](#)
- [Using IronPort Spam Quarantine GUI Logs, page 5-30](#)
- [Using IronPort LDAP Debug Logs, page 5-31](#)
- [Using Safelist/Blocklist Logs, page 5-32](#)
- [Using Reporting Logs, page 5-33](#)
- [Using Reporting Query Logs, page 5-34](#)
- [Using Updater Logs, page 5-35](#)
- [Understanding Tracking Logs, page 5-36](#)
- [Using Authentication Logs, page 5-37](#)

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

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.

These logs do not require any special configuration. However, you must configure the system properly to view attachment names, and attachment names may not always be logged. For information, see [Enabling and Disabling Local Message Tracking, page 3-2](#) and [Tracking Service Overview, page 3-1](#).

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 Cisco IronPort Spam quarantine. It is used to track messages as they are sent to and from the Cisco 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.”
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 5XX 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
```

Message with Attachment

In this example, a content filter with condition “Message Body Contains” has been configured to enable identification of attachment names:

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes

Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0

Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28

Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>

Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>

Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'

Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'

Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>

Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Sat Apr 23 05:05:42 2011 Info: ICID 28 close

Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative

Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative

Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'

Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'

Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'

Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

Note that the second of the three attachments is Unicode. On terminals that cannot display Unicode, these attachments are represented in quoted-printable format.

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 antispm
```

```
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 Cisco 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 Cisco 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.pemailer44.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 Cisco. 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. $\text{del_time} - \text{inj_time}$ = 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
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 [Logging Message Headers, page 5-43](#)), 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.ajsdf1@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@sampldomain.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@sampldomain.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

Table 5-11 Bounce Log Statistics (continued)

Statistic	Description
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 5-43](#)), 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:
```

```
<lu5jak$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
SftBncEvt	Soft Bounced Events
CmpRcp	Completed Recipients
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

Table 5-13 Status Log Statistics (continued)

Statistic	Description
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.
SwPglIn	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 Cisco IronPort Spam quarantine
EuqRis	Estimated number of messages in the Cisco 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\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=recipientsin&height=19
0 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 Scanning Logs

The scanning log contains all LOG and COMMON messages for the appliance's scanning engines. See the Alerts section of the "System Administration" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for a list of available the COMMON and LOG alert messages.

Table 5-21 Scanning Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted
Message	The message consists of an application fault, sent alert, failed alert, or log error message for one of the scanning engines.

Scanning Log Example

In this example, the log shows the history of an appliance sending a warning alert concerning Sophos anti-virus.

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...' (attempt #0).
```

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...'.
```

```
Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com
with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
database on this system is...".
```

Using IronPort Anti-Spam Logs

Table 5-22 *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 5-23 *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 5-24 *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 5-25 *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 5-26 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.d00002b.loc@ldap.rou
oute.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.d00002b.loc@ldap.ro
ute.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 5-27 *Detail of LDAP Debug Log Example*

Line Number	Description
1.	The log file is initialized.
2.	The listener is configured to use LDAP for masquerading, specifically with the LDAP query named "sun.masquerade."
3.	
4.	
	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 <code>ldapflush</code> .
6.	A query is about to be sent to sun.qa, port 389. The query template is: <code>(&(ObjectClass={g})(mailLocalAddress={a}))</code> .
	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.	Now the substitution (described previously) takes place, and this is what the query looks like before it is sent to the LDAP server.
8.	
9.	The connection to the server is not yet established, so make a connection.
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 5-28 shows the statistics recorded in safelist/blocklist logs.

Table 5-28 *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 5-29 shows the statistics recorded in reporting logs.

Table 5-29 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 5-30 shows the statistics recorded in reporting query logs.

Table 5-30 *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 5-31 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 Cisco. 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 5-32 **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.
```

Using Configuration History Logs

A configuration history log consists of a configuration file with an additional section listing the name of the user, a description of where in the configuration the user made changes, and the comment the user entered when committing the change. Each time a user commits a change, a new log is created containing the configuration file after the change.

Configuration History Log Example

In this example, the configuration history log shows that the user (admin) added a guest user to the table that defines which local users are allowed to log in to the system.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<!--

XML generated by configuration change.

Change comment: added guest user
```

User: admin

Configuration are described as:

This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160

Version: 6.7.0-231

Serial Number: 000000000ABC-D0000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"

Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>

Log Subscriptions

This section contains the following topics:

- [Configuring Log Subscriptions, page 5-39](#)
- [Creating a Log Subscription in the GUI, page 5-40](#)
- [Configuring Global Settings for Logging, page 5-42](#)
- [Rolling Over Log Subscriptions, page 5-44](#)
- [Configuring Host Keys, page 5-49](#)

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 retrieved or delivered (pushed) to another computer. Generally, log subscriptions have the following attributes:

Table 5-33 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 2 for more information.
Name	Nickname for the log subscription to be used for your future reference.
Rollover by File Size	The maximum size the file can reach before rolling over.
Rollover by Time	Sets the time interval for file rollovers.
Log level	Sets the level of detail for each log subscription.
Retrieval method	Defines how the log subscription will be obtained from 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.

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 5-34 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.”

Table 5-34 **Log Levels (continued)**

Log Level	Description
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:

Log Name:
(will be used to name the log directory)

File Name:

Rollover by File Size: Maximum
(Add a trailing K or M to indicate size units)

Rollover by Time:

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:
☒ Manually download logs from data.com
Logs are always available via HTTP(S) download. They are also available via SCP if SSH is enabled and FTP if it is enabled on any interface.
Maximum Files:
The maximum number of files retained on the appliance.
☐ FTP Push to Remote Server
FTP Host:
Directory:
Username:
Password:
☐ SCP Push to Remote Server
Protocol: ☐ SSH1 ☒ SSH2
SCP Host: SCP Port:
Directory:
Username:
☐ Enable Host Key Checking
☒ Automatically Scan
☐ Enter Manually

☐ Syslog Push
Hostname:
Protocol: ☒ UDP ☐ TCP
Facility:

- 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 before AsyncOS rolls over the log file as well as a time interval between rollovers. See [Rolling Over Log Subscriptions, page 5-44](#) for more information on rolling over log files.
- Step 4** Select the log level. The available options are Critical, Warning, Information, Debug, or Trace.
- Step 5** Configure the log retrieval method.
- Step 6** Submit and commit your changes.

Editing Log Subscriptions

To edit a log subscription:

- Step 1** Click the name of the log in the Log Settings 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, Cisco 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 Cisco 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 5-35 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

- 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

To prevent log files on the appliance from becoming too large, AsyncOS performs a “rollover” and archives a log file when it reaches a user-specified maximum file size or time interval and creates a new file for incoming log data. Based on the retrieval method defined for the log subscription, the older log file is stored on the appliance for retrieval or delivered to an external computer. See [Log Retrieval Methods, page 5-6](#) for more information on how to retrieve log files from the appliance.

When AsyncOS rolls over a log file, it performs the following actions:

- Renames the current log file with the timestamp of the rollover and a letter “s” extension signifying saved.
- Creates a new log file and designates the file as current with the “**current**” extension.
- Transfers the newly saved log file to a remote host (if using the push-based retrieval method).
- Transfers any previously unsuccessful log files from the same subscription (if using the push-based retrieval method).
- Deletes the oldest file in the log subscription if the total number of files to keep on hand has been exceeded (if using the poll-based retrieval method).

You define a log subscription’s rollover settings when creating or editing the subscription using the System Administration > Log Subscriptions page in the GUI or the `logconfig` command in the CLI. The two settings available for triggering a log file rollover are:

- A maximum file size.
- A time interval.

[Figure 5-3](#) shows the rollover settings available for log subscriptions in the GUI.

Figure 5-3 Log File Rollover Settings for Log Subscriptions

Rollover By File Size

AsyncOS rolls over log files when they reach a maximum file size to prevent them from using too much disk space. When defining a maximum file size for rollovers, use the suffix `m` for megabytes and `k` for kilobytes. For example, enter `10m` if you want AsyncOS to roll over the log file when it reaches 10 megabytes.

Rollover By Time

If you want to schedule rollovers to occur on a regular basis, you can select one of the following time intervals:

- **None.** AsyncOS only performs a rollover when the log file reaches the maximum file size.
- **Custom Time Interval.** AsyncOS performs a rollover after a specified amount of time has passed since the previous rollover. To create a custom time interval for scheduled rollovers, enter the number of days, hours, and minutes between rollovers using `d`, `h`, and `m` as suffixes.
- **Daily Rollover.** AsyncOS performs a rollover every day at a specified time. If you choose a daily rollover, enter the time of day you want AsyncOS to perform the rollover using the 24-hour format (HH:MM).

Only the GUI offers the Daily Rollover option. If you want to configure a daily rollover using the `logconfig` command in the CLI, choose the Weekly Rollover option and use an asterisk (*) to specify that AsyncOS should perform the rollover on every day of the week.

- **Weekly Rollover.** AsyncOS performs a rollover on one or more days of the week at a specified time. For example, you can set up AsyncOS to rollover the log file every Wednesday and Friday at midnight. To configure a weekly rollover, choose the days of the week to perform the rollover and the time of day in the 24-hour format (HH:MM).

If you are using the CLI, you can use a dash (-) to specify a range of days, an asterisk (*) to specify every day of the week, or a comma (,) to separate multiple days and times.

Figure 5-4 shows the settings available for the Weekly Rollover option in the GUI

Figure 5-4 Weekly Log Rollover Settings in the GUI

Table 5-36 shows how to use the CLI to roll over the files for a log subscription on Wednesday and Friday at midnight (00:00).

Table 5-36 *Weekly Log Rollover Settings in the CLI*

```

Do you want to configure time-based log files rollover? [N]> y

Configure log rollover settings:

1. Custom time interval.

2. Weekly rollover.

[1]> 2

1. Monday

2. Tuesday

3. Wednesday

4. Thursday

5. Friday

6. Saturday

7. Sunday

Choose the day of week to roll over the log files. Separate multiple days with comma,
or use "*" to specify every day of a week. Also you can use dash to specify a range
like "1-5":

[ ]> 3, 5

Enter the time of day to rollover log files in 24-hour format (HH:MM). You can specify
hour as "*" to match every hour, the same for minutes. Separate multiple times of day
with comma:

[ ]> 00:00

```

Rolling Over Log Subscriptions on Demand

To roll over log subscriptions immediately using the GUI:

-
- Step 1** On the System Administration > 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.

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 HTTP or HTTPS service enabled on the Management interface in order to view logs via the GUI.

Figure 5-5 *Configuring Log Subscriptions Global Settings*
Log Subscriptions

Configured Log Subscriptions					
Add Log Subscription...					
Log Settings	Type	Log Files	Rollover Interval	All <input type="checkbox"/> Rollover	Delete
antispam	Anti-Spam Logs	antispam/	None	<input type="checkbox"/>	
antivirus	Anti-Virus Logs	antivirus/	None	<input type="checkbox"/>	
asarchive	Anti-Spam Archive	asarchive/	None	<input type="checkbox"/>	
authentication	Authentication Logs	authentication/	None	<input type="checkbox"/>	
avarchive	Anti-Virus Archive	avarchive/	None	<input type="checkbox"/>	
bounces	Bounce Logs	bounces/	None	<input type="checkbox"/>	
cli_logs	CLI Audit Logs	cli_logs/	None	<input type="checkbox"/>	
encryption	Encryption Logs	encryption/	None	<input type="checkbox"/>	
error_logs	IronPort Text Mail Logs	error_logs/	None	<input type="checkbox"/>	
euq_logs	Spam Quarantine Logs	euq_logs/	None	<input type="checkbox"/>	
euqgui_logs	Spam Quarantine GUI Logs	euqgui_logs/	None	<input type="checkbox"/>	
ftpd_logs	FTP Server Logs	ftpd_logs/	None	<input type="checkbox"/>	
gui_logs	HTTP Logs	gui_logs/	None	<input type="checkbox"/>	
mail_logs	IronPort Text Mail Logs	mail_logs/	None	<input type="checkbox"/>	
reportd_logs	Reporting Logs	reportd_logs/	None	<input type="checkbox"/>	
reportqueryd_logs	Reporting Query Logs	reportqueryd_logs/	None	<input type="checkbox"/>	
scanning	Scanning Logs	scanning/	None	<input type="checkbox"/>	
slbld_logs	Safe/Block Lists Logs	slbld_logs/	None	<input type="checkbox"/>	
snmp_logs	SNMP Logs	snmp_logs/	None	<input type="checkbox"/>	
sntpd_logs	NTP logs	sntpd_logs/	None	<input type="checkbox"/>	
status	Status Logs	status/	None	<input type="checkbox"/>	
syslogs	System Logs	syslogs/	None	<input type="checkbox"/>	
system_logs	System Logs	system_logs/	None	<input type="checkbox"/>	
trackerd_logs	Tracking Logs	trackerd_logs/	None	<input type="checkbox"/>	
updater_logs	Updater Logs	updater_logs/	None	<input type="checkbox"/>	
					Rollover Now

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: Manual Download
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download
4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download
6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download
8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download
11. "euggui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download
13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual Download
17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download
19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download
20. "status" Type: "Status Logs" Retrieval: Manual Download
21. "system_logs" Type: "System Logs" Retrieval: Manual Download
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download
23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download

Enter the number of the log you wish to tail.

[]> 19

Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for Quarantine Delivery Host

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs config

Mon Feb 21 23:46:06 2011 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 Cisco 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 8-44](#).

The `hostkeyconfig` subcommand performs the following functions:

Table 5-37 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.

Table 5-37 Managing Host Keys - List of Subcommands

Command	Description
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.
- 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
```




CHAPTER 6

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, page 6-1](#)
- [Monitoring Via the CLI, page 6-6](#)
- [Managing the Email Queue, page 6-24](#)
- [SNMP Monitoring, page 6-39](#)

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 <code>resetcounters</code> 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 <code>/dev/null</code> 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.
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 <code>bouncerecipients</code> command.
Delivered Recipients	Message successfully delivered to a recipient.
Deleted Recipients	Total of message recipients explicitly deleted via the <code>deleterecipients</code> 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 .

Table 6-1 **Counters (continued)**

Statistic	Description
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).
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 <code>LogUsed</code> in the status logs and <code>log_used</code> 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.
Destinations in Memory	<p>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 <code>tophosts</code> 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.”</p> <p>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).</p>
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 <i>overestimate</i> 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 Cisco 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, page 6-7](#)
- [Monitoring Detailed Email Status, page 6-9](#)
- [Monitoring the Status of a Mail Host, page 6-12](#)
- [Determining the Make-up of the Email Queue, page 6-16](#)
- [Displaying Real-time Activity, page 6-17](#)
- [Monitoring Inbound Email Connections, page 6-20](#)
- [Checking the DNS Status, page 6-22](#)
- [Resetting Email Monitoring Counters, page 6-23](#)

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 6-1](#).

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.
System status	Online, offline, receiving suspended, or delivery suspended. Note that the status will be “receiving suspended” only when <i>all</i> listeners are suspended. The status will be “offline” when receiving and delivery are suspended for <i>all</i> 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 <code>featurekey</code> 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 6-1](#).

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 - 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
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 6-1](#).

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 <code>hoststatus</code> field of the same name — tracked per Virtual Gateway address.
Last Activity	Same definition as global <code>hoststatus</code> field of the same name — tracked per Virtual Gateway address.
Recipients	This field also corresponds to the same definition as the global <code>hoststatus</code> 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:
```

```
=====
```

```
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 6-1](#).

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 6-9](#).)

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.

Table 6-8 Data in the hostrate Command

Statistic	Description
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	CrtCncOut	ActvRcp	ActvRcp	DlvRcp	HrdBncRcp	SftBncEvt
	Status			Delta	Delta	Delta	Delta
23:38:23	up	1	0	0	4	0	0
23:38:24	up	1	0	0	4	0	0
23:38:25	up	1	0	0	12	0	0
^C							

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

```

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.

Table 6-10 Data in the *dnsstatus* Command (continued)

Statistic	Description
Cache Exceptions	A request to the DNS cache where the record was found but the domain was unknown.
	A request to the DNS cache where the record was found in the cache, considered for use, and discarded because it was too old.
Cache Expired	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 2-38](#).

Example

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

```
Counters reset: Mon Jan 01 12:00:01 2003
```

Managing the Email Queue

Cisco 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 Cisco IronPort appliance in an offline state or suspended delivery (see [Placing the Cisco IronPort Appliance into a Maintenance State, page 8-2](#)).

**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 Cisco IronPort appliance in an offline state or suspended delivery (see [Placing the Cisco IronPort Appliance into a Maintenance State, page 8-2](#)).

**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 Cisco 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.

Redirecting Messages in Queue

The `redirectrecipients` commands allow you to redirect all messages in the email delivery queue to another relay host. Please note that redirecting recipients to a host or IP address that is not prepared to accept large volumes of SMTP mail from this host will cause messages to bounce and possibly result in the loss of mail.

**Warning**

Redirecting messages to a receiving domain that has /dev/null as its destination results in the loss of messages. The CLI does not display a warning if you redirect mail to such a domain. Check the SMTP route for the receiving domain before redirecting messages.

Example

The following example redirects all mail to the example2.com host.

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

Please enter the hostname or IP address of the machine you want to send all mail to.

```
[> example2.com
```

```
WARNING: redirecting recipients to a host or IP address that is not prepared to accept  
large volumes of SMTP mail from this host will cause messages to bounce and possibly  
result in the loss of mail.
```

```
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
```

```
Redirecting messages, please wait.
```

```
246 recipients redirected.
```

Showing Messages Based on Recipient in Queue

Use the `showrecipients` command to show messages from the email delivery queue by recipient host or Envelope From address. You can also show all messages in the queue.

Example

The following example shows messages in the queue for all recipient hosts.

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

Please select how you would like to show messages:

1. By recipient host.
2. By Envelope From address.
3. All.

```
[1]> 3
```

```
Showing messages, please wait.
```

MID/	Bytes/	Sender/	Subject
[RID]	[Atmps]	Recipient	
1527	1230	user123456@ironport.com	Testing
[0]	[0]	9554@example.com	
1522	1230	user123456@ironport.com	Testing
[0]	[0]	3059@example.com	
1529	1230	user123456@ironport.com	Testing
[0]	[0]	7284@example.com	
1530	1230	user123456@ironport.com	Testing
[0]	[0]	8243@example.com	
1532	1230	user123456@ironport.com	Testing
[0]	[0]	1820@example.com	
1531	1230	user123456@ironport.com	Testing
[0]	[0]	9595@example.com	
1518	1230	user123456@ironport.com	Testing
[0]	[0]	8778@example.com	
1535	1230	user123456@ironport.com	Testing
[0]	[0]	1703@example.com	

```
1533      1230      user123456@ironport.com Testing
[0]       [0]       3052@example.com

1536      1230      user123456@ironport.com Testing
[0]       [0]       511@example.com
```

Suspending Email Delivery

To temporarily suspend email delivery for maintenance or troubleshooting, use the `suspenddel` command. The `suspenddel` command puts Cisco 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**

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 Cisco 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 `resumelister` 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 `resumelistener` command returns Cisco 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.

```
[1]> 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 [Table 6-2 on page 6-4](#) 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 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 Cisco 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 Cisco IronPort AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). This includes Cisco'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

Cisco 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 Cisco 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 Cisco 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 Cisco 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

Table 6-11 Number of Hardware Objects per Cisco IronPort Appliance

Model	CPU Temp	Ambient Temp	Backplane Temp	Riser Temp	Fans	Power Supply Status	Disk Status	NIC Link
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 Cisco 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.
```

```
[1]> setup
```

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

```
Please choose an IP interface for SNMP requests.
```

```
1. Data 1 (192.168.1.1/24: 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**

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>
```




CHAPTER 7

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 Cisco IronPort AsyncOS command syntax.

This chapter contains the following sections:

- [The Cisco IronPort Graphical User Interface \(GUI\), page 7-1](#)
- [Debugging Mail Flow Using Test Messages: Trace, page 7-6](#)
- [Gathering XML status from the GUI, page 7-16](#)

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 Cisco IronPort C150/160 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 [Working with User Accounts, page 8-12](#)) 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]>
```

```
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
```

```
IPv4 Address (Ex: 192.168.1.2):
```

```
[192.168.1.1]>
```

```
Netmask (Ex: "255.255.255.0" or "0xffffffff00"):
```

```
[24]>
```

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:

1. Data 1
2. Data 2
3. Management

[1]>

Hostname:

[mail3.example.com]>

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 FTP 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 Cisco 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. This can be an Internet Protocol version 4 (IPv4) or version 6 (IPv6) address. Note: The <code>trace</code> command prompts for an IP address and a fully-qualified domain name. It does <i>not</i> attempt to reverse the IP address to see if it matches the fully-qualified domain name. The <code>trace</code> 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.	<code>203.45.98.109</code> <code>2001:0db8:85a3::8a2e:0370:7334</code>
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.	<code>smtp.example.com</code>
Listener to Trace Behavior on	Choose from the list of listeners configured on the system to emulate sending the test message to.	<code>InboundMail</code>

Table 7-1 **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 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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> 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	<p>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.</p> <p>If the Cisco IronPort appliance was configured to reject the connection (either through a REJECT or TCPREFUSE access rule), the <code>trace</code> command exits at the point in the processing.</p> <p>For more information on setting HAT parameters, see “Configuring the Gateway to Receive Email” in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>

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	<p>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.</p> <p>For more information, see “SMTP Address Parsing Options” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Masquerading	<p>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 <code>listenerconfig -> edit -> masquerade -> config</code> subcommands.</p> <p>For more information, see “Configuring Masquerading” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

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.

Table 7-2 Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Default Domain	<p>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.</p> <p>For more information, see “SMTP Address Parsing Options” in the “Customizing Listeners” chapter of the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Domain Map Translation	<p>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.</p> <p>For more information, see “The Domain Map Feature” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Recipient Access Table (RAT)	<p>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.)</p> <p>For more information on specifying recipients you accept, see “Accepting Email for Local Domains or Specific Users on Public listeners (RAT)” in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>
Alias Table	<p>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.</p> <p>For more information, see “Creating Alias Tables” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

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 7-2 Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Virtual Gateways	<p>The <code>altsrchost</code> 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 <code>altsrchost</code> command, that information is printed in this section.</p> <p>Note that the virtual gateway address assigned at this point may be overridden by message filter processing below.</p> <p>For more information, see "Using Virtual Gateway™ Technology" in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Bounce Profiles	<p>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.</p> <p>For more information, see "Handling Undeliverable Email" in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

Table 7-2 Viewing Output After Performing a Trace (continued)

trace Command Section	Output
Work Queue Operations	
<p>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 <code>status</code> and <code>status detail</code> commands.</p>	
Masquerading	<p>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 <code>listenerconfig -> edit -> masquerade -> config</code> subcommands.</p> <p>For more information, see “Configuring Masquerading” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
LDAP Routing	<p>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.</p> <p>For more information, see “LDAP Queries” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Message Filters Processing	<p>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 <code>else</code> clause, those actions are evaluated instead. The results of the message filters, processed in order, are printed in this section.</p> <p>See “Using Message Filters to Enforce Email Policies,” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

Mail Policy Processing

The mail policy processing section displays the Anti-Spam, Anti-Virus, Outbreak Filters 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	<p>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 <code>trace</code> command processing stops.</p> <p>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.</p> <p>See “Anti-Spam” in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.</p>
Anti-Virus	<p>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 <code>trace</code> command processing stops.</p> <p>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.</p> <p>See “Anti-Virus” in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.</p>
Outbreak Filters Processing	<p>This section notes messages that contain attachments are to bypass the Outbreak Filters feature. If messages are to be processed by the 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.</p> <p>See “Outbreak Filters” in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.</p>
Footer Stamping	<p>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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>

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 <code>trace</code> command prints “Message Enqueued for Delivery” before this section.	
Global Unsubscribe per Domain and per User	<p>If any recipients you specified as input for the <code>trace</code> 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.</p> <p>See “Using Global Unsubscribe” in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
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*
Trace

Message Definition	
Sender Information	
Source IP:	<input type="text" value="1.2.3.4"/>
Fully Qualified Domain Name of the Source IP: ?	<input type="text" value="remotehost.example.com"/>
Listener to Trace Behavior on:	<input type="button" value="Public (172.22.85.1:25)"/> ▼
SenderBase Network Owner ID:	<input checked="" type="radio"/> Lookup network owner ID associated with source IP <input type="radio"/> Use: <input type="text"/>
SenderBase Reputation Score (SBRS):	<input checked="" type="radio"/> Lookup SBRS associated with source IP <input type="radio"/> Use: <input type="text"/>
Envelope Information	
Envelope Sender:	<input type="text" value="pretend.sender@example.domain"/>
Envelope Recipients (separated by commas):	<input type="text" value="admin@ironport.com"/>
Message Body	
Upload Message Body:	<input type="text"/> <input type="button" value="Browse..."/>
Paste Message Body: (If no file is uploaded.)	<div>Subject: hello</div> <div>This is a test message.</div>

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		

Output for the Trace Page (2 of 2)

Done

Gathering XML status from the GUI

- View status through XML pages, or access XML status information programmatically.

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	<code>http://hostname/xml/status</code>
Host Mail Status for a Specified Host	<code>http://hostname/xml/hoststatus?hostname=host</code>
DNS Status	<code>http://hostname/xml/dnsstatus</code>

GUI Page Name	Corresponding XML status URL
Top Incoming Domains	<code>http://hostname/xml/topin</code>
Top Outgoing Domains ^a	<code>http://hostname/xml/tophosts</code>

^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`.



CHAPTER 8

Common Administrative Tasks

The Framemaker Template contains the following contents:

- [Management of the Cisco IronPort Appliance, page 8-1](#)
- [Support Commands, page 8-6](#)
- [Working with User Accounts, page 8-12](#)
- [Managing Custom User Roles for Delegated Administration, page 8-26](#)
- [Managing the Configuration File, page 8-36](#)
- [Managing Secure Shell \(SSH\) Keys, page 8-44](#)

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:

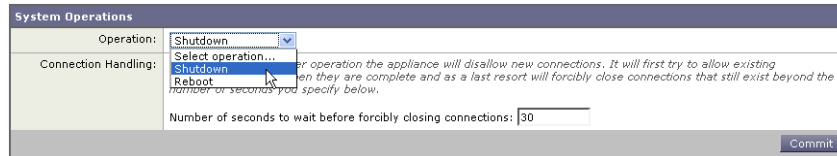
- shutdown
- reboot
- suspend
- offline
- resume
- resetconfig
- version
- updateconfig
- upgrade

Shutting Down the Cisco IronPort Appliance

To shut down your Cisco 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 Cisco 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. Cisco 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

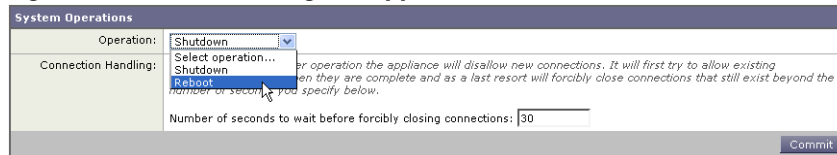


Rebooting the Cisco IronPort Appliance

To reboot your Cisco 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 Cisco 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. Cisco 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 Cisco 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 Cisco 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. Cisco 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*

Mail Operations			
Receiving:	Listener	Suspend (Check All)	Resume (Check All)
	IncomingMail	Suspended	<input type="checkbox"/>
Delivery:	All Mail	Offline	<input type="checkbox"/>
Connection Handling:	<small>When you execute suspend, the appliance will disallow new connections. It will first try to allow existing connections to close when they are complete and as a last resort will forcibly close connections that still exist beyond the number of seconds you specify below.</small>		
	Number of seconds to wait before forcibly closing connections: <input type="text" value="30"/>		
Commit			

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 Cisco 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* Cisco 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 [System Status, page 2-38](#)), 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 Cisco IronPort customer support remote access to your Cisco IronPort appliance.

Figure 8-4 **The Remote Access Page**
Edit Customer Support Remote Access

Customer Support Remote Access	
<input checked="" type="checkbox"/> Allow remote access to this appliance	
Customer Support Password:	<input type="password"/> <small>Cannot be the same as your admin password</small>
Secure Tunnel (recommended):	<input checked="" type="checkbox"/> Initiate connection via secure tunnel Port: <input type="text" value="25"/>
Appliance Serial Number:	XXXXXXXXXXXX-XXXXXXX

By enabling Remote Access you are activating a special account used by Cisco IronPort Customer Support for debugging and general access to the system. This is used by Cisco 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`, Cisco IronPort Customer Support can 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 Cisco 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**
Support Request

Request Technical Support	
Sent Request to:	<input checked="" type="checkbox"/> IronPort Customer Support Other recipients (optional): <input type="text"/> <small>Separate multiple email addresses with commas.</small>
Contact Information:	Name: <input type="text"/> Email: <input type="text"/> Other Contact Information (optional) <input type="text"/> Phone1: <input type="text"/> Phone2: <input type="text"/> <small>(Mobile, Pager, etc.)</small> Other: <input type="text"/>
Issue Description:	Please describe the issue in the space provided below. Provide as much detail as possible to aid in diagnosing the issue. <div style="border: 1px solid black; height: 100px; width: 100%;"></div>
Customer Support Ticket Number (optional):	If you have an existing Customer Support ticket open for this issue, please enter it below. <input type="text"/>

-
- 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 Cisco 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 [Cisco IronPort Customer Support, page 1-4](#).

Packet Capture

Sometimes when you contact Cisco 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 to the `captures` subdirectory, which is also accessible via FTP or SCP. 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 Cisco 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

Current Packet Capture	
No packet capture in progress	
Start Capture	

Manage Packet Capture Files	
C350-005056AA1E14-20100219-200904.cap (61K)	
Delete Selected Files Download File	

Packet Capture Settings	
Capture File Size Limit:	200 MB
Capture Duration:	Run Capture Indefinitely
Interfaces Selected:	ALL
Filters Selected:	(tcp port 25)
Edit Settings...	



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	<p>Choose how long to run the packet capture:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • Run Capture Indefinitely. The packet capture runs until you manually stop it. <p>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.</p> <p>You can always manually stop any packet capture.</p>
Interface	Select the network interface on which to run the packet capture.
Filters	<p>Choose whether or not to apply a filter to the packet capture to reduce the amount of data stored in the packet capture.</p> <p>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 <code>tcpdump</code> command, such as <code>host 10.10.10.10 && port 80</code>.</p> <p>The client IP is the IP address of the machine connecting to the appliance, such as a mail client sending messages through the Email Security appliance.</p> <p>The server IP is the IP address of the machine to which the appliance is connecting, such as an Exchange server to which the appliance is delivering messages.</p> <p>You can use the client and server IP addresses to track traffic between a specific client and a specific server, with the Email Security appliance in the middle.</p>

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

Packet Capture Settings

Capture File Size Limit: MB Maximum file size is 200MB

Capture Duration:

- ☐ Run Capture Until File Size Limit Reached
- ☐ Run Capture Until Time Elapsed Reaches (e.g. 120s, 5m 30s, 4h)
- ☒ Run Capture Indefinitely

The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.

Interfaces:

- ☐ Use selected interfaces
 - ☐ Management
- ☒ Use all interfaces

Packet Capture Filters

Filters: All filters are optional. Fields are not mandatory.

- ☐ No Filters
- ☒ Predefined Filters ?
 - Ports:
 - Client IP:
 - Server IP:
- ☐ Custom Filter ?

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*
Feature Key Settings

Feature Key Settings

Automatic Serving of Feature Keys: ? ☒ Check for and Download Automatically
☒ Activate Feature Keys Automatically

Figure 8-9 *The Feature Keys Page*
Feature Keys

Feature Keys for Serial Number:

Description	Status	Time Remaining	Expiration Date
RSA Email Data Loss Prevention	Active	29 days	26 Nov 16:56 (GMT)
Bounce Verification	Active	30 days	26 Nov 16:57 (GMT)
IronPort Email Encryption	Active	30 days	26 Nov 16:57 (GMT)
IronPort Anti-Spam	Active	30 days	26 Nov 16:57 (GMT)
Incoming Mail Handling	Active	30 days	26 Nov 16:57 (GMT)
Virus Outbreak Filters	Active	30 days	26 Nov 16:57 (GMT)
Sophos Anti-Virus	Active	30 days	26 Nov 16:57 (GMT)
McAfee	Active	30 days	26 Nov 16:57 (GMT)

Pending Activation

No feature key activations are pending.

Feature Activation

Feature Key:

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 Cisco 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 Cisco IronPort representative or support organization.

Working with User Accounts

The Cisco IronPort appliance provides two methods for adding user accounts: creating user accounts on the Cisco 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 8-23](#).

The default user account for the system, `admin`, has all administrative privileges. The `admin` user account cannot be deleted, but you can change the password and lock the account.

When you create a new user account, you assign the user to a predefined or a custom user role. Each role contains differing levels of permissions within the system.

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.”

[Table 8-2](#) defines the roles available for user accounts.

Table 8-2 **User Roles Listing**

User Role	Description
Administrator	<p>User accounts with the Administrator role have full access to all configuration settings of the system. However, only the <code>admin</code> user has access to the <code>resetconfig</code> and <code>revert</code> commands.</p> <p>Note AsyncOS does not support multiple administrators configuring the Email Security appliance from the GUI simultaneously.</p>
Technician	<p>User accounts with the Technician role can perform system upgrades, reboot the appliance, and manage feature keys. Technicians can also perform the following actions in order to upgrade the appliance:</p> <ul style="list-style-type: none"> • Suspend email delivery and receiving. • View status of workqueue and listeners. • Save and email configuration files. • Back up safelists and blocklists. Technicians cannot restore these lists. • Disconnect the appliance from a cluster. • Enable or disable remote service access for Cisco IronPort technical support. • Raise a support request.
Operator	<p>User accounts with the Operator role are restricted from:</p> <ul style="list-style-type: none"> • Creating or editing user accounts. • Issuing the <code>resetconfig</code> command. • Issuing the <code>systemsetup</code> command or running the System Setup Wizard. • Issuing the <code>adminaccessconfig</code> command. • Performing some quarantine functions (including creating and deleting quarantines). • Modifying LDAP server profile settings other than username and password, if LDAP is enabled for external authentication. <p>Otherwise, they have the same privileges as the Administrator role.</p>

Table 8-2 **User Roles Listing**

User Role	Description
Guest	Users accounts with the Guest role can only view status information. Users with the Guest role can also manage messages in the Cisco IronPort Spam Quarantine and system quarantines, if access is enabled. Users with the Guest role cannot access Message Tracking.
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 Cisco 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: <ul style="list-style-type: none"> • Message tracking. • Managing the Cisco 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 Cisco IronPort Spam Quarantine and system quarantines before a user with this role can manage them.
Custom user role	User accounts with a custom user role can only access email security features assigned to the role. These features can be any combination of DLP policies, email policies, reports, quarantines, local message tracking, encryption profiles, and the Trace debugging tool. The users cannot access system configuration features. Only administrators can define custom user roles. See Managing Custom User Roles for Delegated Administration, page 8-26 for more information. Note Users assigned to custom roles cannot access the CLI.

All roles defined in [Table 8-2](#) can access both the GUI and the CLI, except the Help Desk User role and custom user roles, which can only access the GUI.

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 8-23](#).

Managing Users

You can manage users on the System Administration > Users page.

Figure 8-10 **The Users Page**
Users

Users

[Add User...](#)

Accounts	User Name	Full Name	User Role	Account Status	Password Expires	Delete
<input type="checkbox"/>	bob1	Bob Jones	Policy Administrator*	Active	n/a	
<input type="checkbox"/>	brad1	Bradley Knight	Help Desk User	Active	n/a	
<input type="checkbox"/>	grace1	Grace Brown	Policy Administrator*	Active	n/a	
<input type="checkbox"/>	jessie1	Jessie Baxter	Quarantine Manager*	Active	n/a	
<input type="checkbox"/>	stephen1	Stephen Graham	Technician	Active	n/a	
<input type="checkbox"/>	susan1	Susan Warner	DLP Administrator*	Active	n/a	
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	

[Reset Passwords](#)

* Custom User Role for delegated administration.

Local User Account & Password Settings

Account Lock:	Not configured.
Password Reset:	Not configured.
Password Rules:	Require at least 6 characters.

[Edit Settings...](#)

External Authentication

External Authentication is disabled.

[Enable...](#)

DLP Tracking Privileges

DLP Tracking Privileges:	Access allowed.
--------------------------	-----------------

[Edit Settings...](#)

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. For more information, see [Adding Users, page 8-15](#).
- Delete users. For more information, see [Deleting Users, page 8-17](#).
- Edit users, such as changing a user's password and locking and unlocking a user's account. For more information, see [Editing Users, page 8-16](#).
- Configure user account and password settings for local accounts. For more information, see [Configuring Restrictive User Account and Password Settings, page 8-20](#).
- Enable the appliance to use an LDAP or RADIUS directory to authenticate users. For more information, see [External Authentication, page 8-23](#) for more information.
- Enable access for non-administrators to DLP Matched Content in Message Tracking. See [Controlling Access to Sensitive Information in Message Tracking, page 8-18](#) for more information.

Adding Users

To add a user:

- Step 1** On the System Administration > Users page, click **Add User**. The Add User page is displayed:

Figure 8-11 Adding a User
Add Local User

The screenshot shows the 'Local User Settings' form. At the top, 'Account Status' is set to 'Active'. Below are input fields for 'User Name' and 'Full Name'. The 'User Role' section has two radio buttons: 'Predefined Roles' (selected) and 'Custom Roles'. Under 'Predefined Roles', a dropdown menu is open showing options: 'Administrator', 'Cloud Guest', 'Cloud Operator', 'DUP Administrator', 'Domain Admin', and 'Policy Administrator'. The 'Password' section has two input fields: 'Password' and 'Retype Password'. To the right of these fields, a note states: 'A password must contain the following: • at least 6 characters.' At the bottom of the form are 'Cancel' and 'Submit' buttons.

- Step 2** Enter a login name for the user. Some words are reserved (such as “operator” or “root”).
- Step 3** Enter the user’s full name.
- Step 4** Select a predefined or custom user role. (See [Table 8-2](#) for more information about user roles.)



Note You can create a new user role and apply it to this user account. See [Managing Custom User Roles for Delegated Administration, page 8-26](#) for more information.

- Step 5** Enter a password and retype it. Passwords must comply with the rules defined in the Local User Account & Password Settings section. See [Configuring Restrictive User Account and Password Settings, page 8-20](#) for more information.
- 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.

Locking and Unlocking a User Account

Locking a user account prevents a local user from logging into the appliance. A user account can be locked in one of the following ways:

- AsyncOS locks a user account if the user exceeded the maximum number of failed login attempts defined in the Local User Account & Password Settings section.
- Administrators can manually lock user accounts for security purposes using the System Administration > Users page.

AsyncOS displays the reason why the user account was locked when you view the user account on the Edit User page.

Figure 8-12 **A Locked User Account**
Edit Local User

Local User Settings

Account Status:	Locked	Unlock Account
Reason: User exceeded maximum number of failed login attempts.		
User Name:	bob1	
Full Name:	Bob Jones	
User Role: ?	<input checked="" type="radio"/> Predefined Roles Operator <input type="radio"/> Custom Roles Add Role... DLP Administrator Policy Administrator Quarantine Manager Unassigned	
Password:	Password: <input type="password"/> Retype Password: <input type="password"/>	
A password must contain the following: • at least 6 characters.		

[Cancel](#) [Submit](#)

To unlock a user account, open the user account by clicking on the user name in the Users listing and click **Unlock Account**.

To manually lock a local user account, open the user account by clicking on the user name in the Users listing and click **Lock Account**. AsyncOS displays a message saying that the user will be unable to log into the appliance and asks if you want to continue.

You can also configure all local user accounts to lock after users fail to login successfully after a configured number of attempts. For more information, see [Configuring Restrictive User Account and Password Settings](#), page 8-20.



Note

If you lock the admin account, you can only be unlocking by logging in as the admin through a serial communications connection to the serial console port. The admin user can always access the appliance using the serial console port, even when the admin account is locked. See the “Setup and Installation” chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information on accessing the appliance using the serial console port.

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.

Controlling Access to Sensitive Information in Message Tracking

Messages that violate Data Loss Prevention (DLP) policies typically include sensitive information, such as corporate confidential information or personal information including credit card numbers and health records. By default, this content appears in the DLP Matched Content tab on the Message Details page for messages listed in Message Tracking results.

You can choose to hide this tab and its content from users who have access to Message Tracking based on their assigned predefined or custom role. Administrator users can always see this content.

To specify which user groups can see this content:

-
- Step 1** Go to the **System Administration > Users** page.
- Step 2** Under **DLP Tracking Privileges**, click **Edit Settings**.
The DLP Tracking Privileges page appears.

Figure 8-13 *DLP Tracking Privileges*
DLP Tracking Privileges

- Step 3** Select the roles for which you want to grant access to DLP data in Message Tracking.
Custom roles without access to Message Tracking can never view this information and thus are not listed.
- Step 4** Submit and commit your changes.

The following features must be enabled in Security Services for this setting to take effect:

- Message Tracking
 - RSA Email DLP
 - RSA Email DLP > Matched Content Logging
-

For more information on DLP policies, see the “Data Loss Prevention” chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide*.

For more information on searching for DLP violations in Message Tracking, see [Running a Search Query, page 3-5](#).

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.

In the CLI, use the `password` or `passwd` command to change your password. If you forget the password for the admin user account, contact your customer support provider to reset the password.

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
=====	=====	=====	=====	=====
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

```

Configuring Restrictive User Account and Password Settings

You can define user account and password restrictions to enforce organizational password policies. The user account and password restrictions apply to local users defined on the Cisco IronPort appliance. You can configure the following settings:

- **User account locking.** You can define how many failed login attempts cause the user to be locked out of the account.
- **Password lifetime rules.** You can define how long a password can exist before the user is required to change the password after logging in.
- **Password rules.** You can define what kinds of passwords users can choose, such as which characters are optional or mandatory.

You define user account and password restrictions on the System Administration > Users page in the Local User Account and Password Settings section.

Figure 8-14 shows the Local User Account and Password Settings section on the Users page.

Figure 8-14 Users Page, Local User Account and Password Settings Section

Local User Account & Password Settings	
Account Lock:	Not configured.
Password Reset:	Not configured.
Password Rules:	Require at least 6 characters.
Edit Settings...	

To configure user account and password restrictions:

-
- Step 1** On the System Administration > Users page, click **Edit Settings** in the Local User Account and Password Settings section. The Local User Account and Password Settings page is displayed.

Figure 8-15 Configuring User Account and Password Restrictions**Local User Account & Password Settings**

Local User Account & Password Settings	
User Account Lock:	<input type="checkbox"/> Lock accounts after <input type="text" value="5"/> failed login attempts.* <input type="checkbox"/> Display Locked Account Message <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> Your account is not available due to administrative action. Please contact your Administrator. </div> <p><small>This message appears on the login page if an Administrator manually locks a user account. If the User Account Lock settings are enabled, the message also appears after too many login attempts occur.</small></p>
Password Reset:	<input type="checkbox"/> Require a password reset whenever a user's password is set or changed by an admin (Recommended). <input type="checkbox"/> Require users to reset passwords after <input type="text" value="90"/> days. <input checked="" type="checkbox"/> Display reminder <input type="text" value="14"/> days before expiration.
Password Rules:	<input checked="" type="checkbox"/> Require at least <input type="text" value="6"/> characters. <input type="checkbox"/> Require at least one upper (A-Z) and one lower (a-z) case letter. <input type="checkbox"/> Require at least one number (0-9). <input type="checkbox"/> Require at least one special character. (?) <input type="checkbox"/> Ban usernames and their variations as passwords. <input type="checkbox"/> Ban reuse of the last <input type="text" value="3"/> passwords.

*Settings do not apply to Admin User.

Step 2 Configure the settings described in [Table 8-3](#).

Table 8-3 Local User Account and Password Settings

Setting	Description
User Account Lock	<p>Choose whether or not to lock the user account after the user fails to login successfully. Specify the number of failed login attempts that cause the account locking. You can enter any number from one (1) to 60. Default is five (5).</p> <p>When you configure account locking, enter the message to be displayed to the user attempting to login. Enter text using 7-bit ASCII characters. This message is only displayed when users enter the correct password to an account locked by an administrator. This message is not shown for accounts locked due to failed login attempts.</p> <p>When a user account gets locked, an administrator can unlock it on the Edit User page in the GUI or using the <code>userconfig</code> CLI command.</p> <p>Failed login attempts are tracked by user, regardless of the machine the user connects from or the type of connection, such as SSH or HTTP. Once the user successfully logs in, the number of failed login attempts is reset to zero (0).</p> <p>When a user account is locked out due to reaching the maximum number of failed login attempts, an alert is sent to the administrator. The alert is set at the “Info” severity level.</p> <p>Note You can also manually lock individual user accounts. For more information see Locking and Unlocking a User Account, page 8-16.</p>

Table 8-3 *Local User Account and Password Settings (continued)*

Setting	Description
Password Reset	<p>Choose whether or not users should be forced to change their passwords after an administrator changes their passwords.</p> <p>You can also choose whether or not users should be forced to change their passwords after they expire. Enter the number of days a password can last before users must change it. You can enter any number from one (1) to 366. Default is 90.</p> <p>When you force users to change their passwords after they expire, you can display a notification about the upcoming password expiration. Choose the number of days before expiration to notify users.</p> <p>After a password expires, the user is forced to change the account password at the next login.</p> <p>Note When a user account uses SSH keys instead of a password challenge, the Password Reset rules still apply. When a user account with SSH keys expires, the user must enter their old password or ask an administrator to manually change the password to change the keys associated with the account. For more information, see Managing Secure Shell (SSH) Keys, page 8-44.</p>
Password Rules: Require at <number> least characters.	<p>Enter the minimum number of characters passwords may contain.</p> <p>You can enter any number from six (6) to 128. Default is six (6).</p>
Password Rules: Require at least one number (0-9).	<p>Choose whether or not the passwords must contain at least one number.</p>
Password Rules: Require at least one special character.	<p>Choose whether or not the passwords must contain at least one special character. Passwords may contain the following special characters:</p> <p>~ ? ! @ # \$ % ^ & * - _ + =</p> <p>\ / [] () < > { } ` ' " ; : , .</p>

Table 8-3 *Local User Account and Password Settings (continued)*

Setting	Description
Password Rules: Ban usernames and their variations as passwords.	Choose whether or not the password are allowed to be the same as the associated username or variations on the username. When username variations are banned, the following rules apply to passwords: <ul style="list-style-type: none"> • The password may not be the same as the username, regardless of case. • The password may not be the same as the username in reverse, regardless of case. • The password may not be the same as the username or reversed username with the following character substitutions: <ul style="list-style-type: none"> – "@" or "4" for "a" – "3" for "e" – "l", "!", or "1" for "i" – "0" for "o" – "\$" or "5" for "s" – "+" or "7" for "t"
Password Rules: Ban reuse of the last <number> passwords.	Choose whether or not users are allowed to choose a recently used password when they are forced to change the password. If they are not allowed to reuse recent passwords, enter the number of recent passwords that are banned from reuse. You can enter any number from one (1) to 15. Default is three (3).

Step 3 Submit and commit your changes.

External Authentication

If you store user information in an LDAP or RADIUS directory on your network, you can configure your Cisco 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 8-16 Enabling External Authentication

Enabling LDAP Authentication

In addition to using an LDAP directory to authenticate users, you can assign LDAP groups to Cisco 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 8-17 Enabling External Authentication Using LDAP
Edit External Authentication

 A screenshot of the 'Edit External Authentication' page. It features a section 'External Authentication Settings' with a checked 'Enable External Authentication' checkbox. Below this, there are fields for 'Authentication Type' (set to LDAP), 'External Authentication Cache Timeout' (0 seconds), 'LDAP External Authentication Query' (LDAP_externalauth), and 'Timeout To Wait For Valid Response From Server' (10 seconds). A 'Group Mapping' table is shown with columns for 'Group Name in Directory', 'Role' (set to Administrator), and an 'Add Row' button. A note at the bottom states 'Group names are case-sensitive.'

- 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 Cisco IronPort roles. The RADIUS server should support the CLASS attribute, which AsyncOS uses to assign users in the RADIUS directory to Cisco 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 Cisco IronPort user roles, first set the CLASS attribute on the RADIUS server with a string value of <radius-group>, which will be mapped to Cisco 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 8-18 Enabling External Authentication Using RADIUS
Edit External Authentication

- 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 Cisco 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 a Cisco IronPort role, or grant all RADIUS users the Administrator role. It is recommended that you map RADIUS groups to Cisco IronPort roles.
 - Step 12** If you chose to map a RADIUS group to a Cisco 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 11 and 12 for each group of users that the appliance authenticates.
 - Step 14** Submit and commit your changes.
-

Managing Custom User Roles for Delegated Administration

You can design custom user roles and delegate specific responsibilities to users that align with their roles within your organization, allowing these *delegated administrators* access only to the email security features they are responsible for and not the system configuration features that are not related to their roles. Delegated administration provides more flexible control over your users' access to the email security features on the appliance than the predefined administrator, operator, and help desk user roles.

For example, you may have users who are responsible for managing mail policies for specific domains on the Email Security appliance, but you do not want these users to access the system administration and security services configuration features, which the predefined administrator and operator roles grant. You can create a custom user role for mail policy administrators who can grant these users access to the mail policies they manage, along with other email security features that they can use to manage messages processed by these policies, such as Message Tracking and policy quarantines.

Use the System Administration > User Roles page in the GUI (or the `userconfig -> role` command in the CLI) to define custom user roles and manage the email security features for which they are responsible, such as mail policies, RSA Email DLP policies, email reports, and quarantines. For a full list of email security features that delegated administrators can manage, see [Assigning Access Privileges, page 8-28](#). Custom roles can also be created when adding or editing a local user account using the System Administration > Users page. See [Defining a Custom User Role When Adding a User Account, page 8-33](#) for more information.

You should make sure when creating a custom user role so that its responsibilities don't overlap too much with the responsibilities of other delegated administrators. If multiple delegated administrators are responsible for the same content filter, for example, and use the content filter in different mail policies, the changes made to the filter by one delegated administrator may cause unintended side effects for the mail policies managed by other delegated administrators.

When you have created the custom user roles, you can assign local users and external authentication groups to them like any other user role. See [Working with User Accounts, page 8-12](#) for more information. Please note that users assigned to custom roles cannot access the CLI.

[Figure 8-19](#) displays a list of custom user roles defined for an Email Security appliance, including the access privileges assigned to the roles.

Figure 8-19 **List of Custom User Roles**
User Roles

Custom User Roles for Delegated Administration										
Add User Role...										
Role Name	Privileges							Assigned Users	Duplicate	Delete
	Email Policies	Data Loss Prevention	Reporting	Message Tracking	Trace	Quarantines	Encryption Profiles			
DLP Administrator	No Access	DLP Policies: 3 	Relevant Reports*	Available	No Access	No Access	Feature Disabled	susan1		
Policy Administrator	Incoming Policies: 1 Content Filters: 0 Outgoing Policies: 1 Content Filters: 0 	No Access	Relevant Reports*	Available	No Access	Quarantines: 1	Feature Disabled	grace1		
Quarantine Manager	No Access	No Access	No Access	No Access	No Access	Quarantines: 3	Feature Disabled	jessie1		

* Report access for this role is controlled by the Mail Policy and DLP privileges.

Key: View restricted to editable items

Account Privileges Page

When a delegated administrator logs into the appliance, the Account Privileges page displays links to the security features for which the delegated administrator is responsible and brief descriptions of their access privileges. A delegated administrator can return to this page by selecting Account Privileges in the Options menu. Delegated administrators can also access the features that they manage using the menu at the top of the web page.

Figure 8-20 shows an Account Privileges page for a delegated administrator with access to mail policies, email reporting, message tracking, and quarantines.

Figure 8-20 Account Privileges Page for a Delegated Administrator
Account Privileges (bob1)

Mail Policies	Incoming Mail Policies (1) Incoming Content Filters (1) Outgoing Mail Policies (1) Outgoing Content Filters (None Assigned) <i>Configure Email Policies and Content Filters.</i>
Email Reporting	Policy Reporting and DLP Reporting <i>View and analyze email traffic.</i>
Message Tracking	Message Tracking <i>Track messages.</i>
Quarantine	Manage Message Quarantines (1) <i>Manage messages in assigned Quarantines.</i>

Assigning Access Privileges

When creating a custom user role, you define the levels of access to the security features for which delegated administrators are responsible.

The security features available for delegated administrators to manage are:

- Incoming and outgoing mail policies and content filters.
- Data Loss Prevention (DLP) policies.
- Email reporting.
- Message Tracking.
- The Trace debugging tool.
- Spam, policy, virus, and outbreak quarantines.
- Cisco IronPort Email Encryption profiles.

Figure 8-21 displays the different access privileges available for these features when creating a custom user role.

Figure 8-21 Access Privileges Available for a Custom User Role
Add User Role

Settings

Name:

Description:

Access Privileges:

Mail Policies and Content Filters: ☒ No access
☐ View assigned, edit assigned
☐ View all, edit all (full access)

DLP Policies: ☒ No access
☐ View assigned, edit assigned
☐ View all, edit assigned
☐ View all, edit all (full access)

Email Reporting: ☒ No access
☐ View relevant reports*
☐ View all reports

Message Tracking: ☒ No access
☐ Message Tracking access

Trace: ☒ No access
☐ Trace access

Quarantines: ☒ No access
☐ Manage assigned quarantines

Encryption Profiles: As assigned

*Access to reports is controlled by Mail Policy and DLP privileges

After defining the access levels for a custom user role, you need to assign the specific mail policies, content filters, DLP policies, quarantines, or encryption profiles for which the delegated administrators will be responsible.

For example, you can create two different DLP policy administrator roles that are responsible for different RSA Email DLP policies. One role is only responsible for DLP violations related to company confidentiality and acceptable use, while the other is responsible for DLP violations related to privacy protection. In addition to DLP policies access, these custom user roles can also be assigned privileges for tracking message data and viewing quarantines and reports. They can search for DLP violations related to the policies that they are responsible for in using Message Tracking.

You can view which responsibilities are available to assign to a custom user role by clicking on the links for the assigned privileges in the Custom User Roles for Delegated Administration table on the User Roles page. See [Updating Responsibilities for a Custom User Role, page 8-34](#).

Mail Policies and Content Filters

The Mail Policies and Content Filters access privileges define a delegated administrator's level of access to the incoming and outgoing mail policies and content filters on the Email Security appliance. You can assign specific mail policies and content filters to a custom user role, allowing only the delegated administrators belonging to this role, along with operators and administrators, to manage the mail policies and content filters.

All delegated administrators with this access privilege can view the default incoming and outgoing mail policies but they can only edit these policies if they have full access.

All delegated administrators with access privileges can create new content filters to use with their mail policies. A content filter created by a delegated administrator is available to the other delegated administrators assigned to the custom user role. Content filters that are not assigned to any custom user role are public and can be viewed by all delegated administrators with the mail policy access privilege. Content filters created by operators and administrators are *public* by default. Delegated administrators can enable or disable any existing content filters on mail policies assigned to their custom user role, but they cannot modify or delete public content filters.

If a delegated administrator deletes a content filter used by mail policies other than their own, or if the content filter is assigned to other custom user roles, AsyncOS does not delete the content filter from the system. AsyncOS instead unlinks the content filter from the custom user role and removes it from the delegated administrator's mail policies. The content filter remains available to other custom user roles and mail policies.

Delegated administrators can use any text resource or dictionary in their content filters, but they cannot access the Text Resources or Dictionaries pages in the GUI to view or modify them. Delegated administrators also cannot create new text resources or dictionaries.

For outgoing mail policies, delegated administrators can enable or disable DLP policies but they cannot customize the DLP settings unless they also have DLP policy privileges.

You can assign one of the following access levels for mail policies and content filters to a custom user role:

- **No access:** Delegated administrators cannot view or edit mail policies and content filters on the Email Security appliance.
- **View assigned, edit assigned:** Delegated administrators can view and edit the mail policies and content filters assigned to the custom user role and create new content filters. Delegated administrators can edit a policy's Anti-Spam, Anti-Virus, and Outbreak Filters settings. They can enable their content filters for the policy, as well as disable any existing content filter assigned to the policy, regardless of whether they are responsible for it. Delegated administrators cannot modify a mail policy's name or its senders, recipients, or groups. Delegated administrators can modify the order of the content filters for mail policies assigned to their custom user role.
- **View all, edit assigned:** Delegated administrators can view all mail policies and content filters on the appliance, but they can only edit the ones assigned to the custom user role.

View all, edit all (full access): Delegated administrators have full access to all of the mail policies and content filters on the appliance, including the default mail policies, and have the ability to create new mail policies. Delegated administrators can modify the senders, recipients, and groups of all mail policies. They can also reorder mail policies.

You can assign individual mail policies and content filters to the custom user role using either the Email Security Manager or the Custom User Roles for Delegated Administration table on the User Roles page.

See the "Email Security Manager" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information on using the Email Security Manager for mail policies and content filters.

See [Updating Responsibilities for a Custom User Role, page 8-34](#) for information on using the Custom User Roles for Delegated Administration table to assign mail policies and content filters.

DLP Policies

The DLP Policies access privileges define a delegated administrator's level of access to the DLP policies via the DLP Policy Manager on the Email Security appliance. You can assign DLP policies to specific custom user roles, allowing delegated administrators, in addition to operators and administrators, to manage these policies. Delegated administrators with DLP access can also export DLP configuration files from the Data Loss Prevention Global Settings page. Only administrators and operators can change the mode of DLP used from RSA Email DLP to RSA Enterprise Manager, and vice versa.

If a delegated administrator also has mail policy privileges, they can customize the RSA Email DLP policies. Delegated administrators can use any custom DLP dictionary for their RSA Email DLP policies, but they cannot view or modify the custom DLP dictionaries.

You can assign one of the following access levels for RSA Email DLP policies to a custom user role:

- **No access:** Delegated administrators cannot view or edit RSA Email DLP policies on the Email Security appliance.
- **View assigned, edit assigned:** Delegated administrators can use the DLP Policy Manager to view and edit the RSA Email DLP policies assigned to the custom user role. Delegated administrators cannot rename or reorder DLP policies in the DLP Policy Manager. Delegated administrators can export DLP configurations.
- **View all, edit assigned:** Delegated administrators can view and edit the RSA Email DLP policies assigned to the custom user role. They can export DLP configurations. They can also view all RSA Email DLP policies that are not assigned to the custom user role but they cannot edit them. Delegated administrators cannot reorder DLP policies in the DLP Policy Manager or rename the policy.
- **View all, edit all (full access):** Delegated administrators have full access to all of the RSA Email DLP policies on the appliance, including the ability to create new ones. Delegated administrators can reorder DLP policies in the DLP Policy Manager. They cannot change the DLP mode that the appliance uses.

You can assign individual RSA Email DLP policies to the custom user role using either the DLP Policy Manager or the Custom User Roles for Delegated Administration table on the User Roles page.

See the “Data Loss Prevention” chapter in the *Cisco IronPort AsyncOS for Email Advanced Configuration Guide* for more information on RSA Email DLP policies and the DLP Policy Manager.

See [Updating Responsibilities for a Custom User Role, page 8-34](#) for information on using the Custom User Roles for Delegated Administration list to assign RSA Email DLP policies.

Email Reporting

The Email Reporting access privileges define which reports and Email Security Monitor pages a delegated administrator can view, depending on the custom user role’s access to mail policies, content filters, and RSA Email DLP policies. These reports are not filtered for assigned policies; delegated administrators can view reports for mail and DLP policies that for which they are not responsible.

You can assign one of the following access levels for email reporting to a custom user role:

- **No access:** Delegated administrators cannot view reports on the Email Security appliance.
- **View relevant reports:** Delegated administrators can view reports on the Email Security Monitor pages related to their Mail Policies and Content Filters and DLP Policies access privileges. Delegated administrators with Mail Policies and Content Filters access privileges can view the following Email Security Monitor pages:
 - Overview
 - Incoming Mail
 - Outgoing Destinations
 - Outgoing Senders
 - Internal Users
 - Content Filters
 - Virus Outbreaks
 - Virus Types
 - Archived Reports

Delegated administrators with DLP Policies access privileges can view the following Email Security Monitor pages:

- Overview
- DLP Incidents
- Archived Reports
- **View all reports:** Delegated administrators can view all reports and Email Security Monitor pages on the Email Security appliance.

See the Chapter 2, “Using Email Security Monitor,” on page 1 chapter for more information on email reporting and the Email Security Monitor.

Message Tracking

The Message Tracking access privileges define whether delegated administrators assigned to the custom user role have access to Message Tracking, including message content that may violate your organization’s DLP policies if the DLP Tracking Policies option has been enabled on the System Administration > Users page and the custom user role also has DLP policies access privileges.

Delegated administrators can only search for the DLP violations for the RSA Email DLP policies assigned to them.

See Chapter 3, “Tracking Email Messages,” on page 1 for more information on Message Tracking.

See [Controlling Access to Sensitive Information in Message Tracking, page 8-18](#) for information for allowing delegated administrators access to viewing matched DLP content in Message Tracking.

Trace

The Trace access privileges define whether delegated administrators assigned to the custom user role can use Trace to debug the flow of messages through the system. Delegated administrators with access can run Trace and view all of the generated output. Trace results are not filtered based on the delegated administrator’s mail or DLP policy privileges.

See [Debugging Mail Flow Using Test Messages: Trace, page 9-1](#) for more information on using Trace.

Quarantines

The Quarantines access privileges define whether delegated administrators can manage assigned quarantines. Delegated administrators can view and take actions on any message in an assigned quarantine, such as releasing or deleting messages, but cannot change the quarantine’s configuration (e.g. the size, retention period, etc.), or create or delete quarantines.

You can assign any of the quarantines to the custom user role using either the Monitor > Quarantines page or the Custom User Roles for Delegated Administration table on the User Roles page.

See Chapter 4, “Quarantines,” on page 1 for more information on Quarantines.

See [Updating Responsibilities for a Custom User Role, page 8-34](#) for information on using the Custom User Roles for Delegated Administration list to assign quarantines.

Encryption Profiles

The Encryption Profiles access privileges define whether delegated administrators can use encryption profiles assigned to their custom user role when editing content filters or DLP policies. Encryption profiles can only be assigned to custom user roles with mail or DLP policy access privileges. Encryption profiles that are not assigned to a custom role are available for use by all delegated administrators with mail or DLP policy privileges. Delegated administrators cannot view or modify any encryption profiles.

You can assign encryption profiles when creating or editing an encryption profile using the Security Services > IronPort Email Encryption page.

See the “Cisco IronPort Email Encryption” chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Defining a Custom User Role

User the User Roles page in the GUI (or the `userconfig -> role` command in the CLI) to define a new user role and assign its access privileges. The User Roles page displays all existing custom user roles on the appliance and the access privileges for each role.

To define a custom user role using the User Roles page:

-
- Step 1** Go to the **System Administration > User Roles** page.
 - Step 2** Click **Add User Role**. The Add User Role page is displayed.
 - Step 3** Enter a name for the user role.
 - Step 4** Enter a description of the user role and its privileges.
 - Step 5** Select the user role’s access privileges. (See [Assigning Access Privileges](#), page 8-28 for more information on each type of access privilege.)
 - Step 6** Submit and commit your changes.
-

Defining a Custom User Role When Adding a User Account

You can create a new custom user role when adding or editing a local user account on the Email Security appliance. [Figure 8-22](#) displays the option available for adding a custom user role on the Add Local User page.

Figure 8-22 Option for Adding a Custom Role When Adding a User Account



See [Managing Users](#), page 8-14 for more information on adding a user account.

To define the custom user role when creating a user account:

-
- Step 1** Go to the **System Administration > Users** page.

- Step 2** Click **Add User**.
- Step 3** When creating the user account, select Custom Roles.
- Step 4** Select **Add Role**.
- Step 5** Enter the name for the new role.
- Step 6** Submit the new user account.
AsyncOS displays a notification that the new user account and custom user role have been added.
- Step 7** Go to the **System Administration > User Roles** page.
- Step 8** Click on the name of the custom user role in the Custom User Roles for Delegated Administration table. The Edit User Role page is displayed.
- Step 9** Enter a description of the user role and its privileges.
- Step 10** Select the user role's access privileges. (See [Assigning Access Privileges](#), page 8-28 for more information on each type of access privilege.)
- Step 11** Submit and commit your changes.

Updating Responsibilities for a Custom User Role

While you can assign responsibilities to custom user roles by browsing to the individual security features using the menu at the top of the GUI, the Custom User Roles for Delegated Administration table on the User Roles page consolidates links to all of the security features that delegated administrators can manage in one place, with the exception of Encryption profiles. Clicking on the name of a custom user group's access privilege in the table displays a list of all the mail policies, content filters, active RSA Email DLP policies, or quarantines on the appliance and displays the names of any other custom user role that has access to them.

For example, [Figure 8-23](#) displays a list of active RSA Email DLP policies available on an Email Security appliance. It also lists another custom user group that has access to the DLP policies. From this list, an administrator can select which DLP policies the delegated administrators using the DLP Policy Manager.

Figure 8-23 DLP Policies Available for Delegated Administrators
User Role: DLP Administrator > DLP Policies

Active DLP Policies for Outgoing Mail			
Include	Order	DLP Policy	Other Roles with Edit Access
<input checked="" type="checkbox"/>	1	Payment Card Industry Data Security Standard (PCI-DSS)	Domain Admin
<input checked="" type="checkbox"/>	2	California SB-1386	Domain Admin
<input type="checkbox"/>	3	Restricted Files	Domain Admin

Cancel

Submit

To update a custom user role's responsibilities:

- Step 1** Go to the **System Administration > User Roles** page.
- Step 2** Click the name of the access privilege for the custom user role you want to update.
AsyncOS displays a list of all the mail policies, content filters, DLP policies, or quarantines available on the appliance, along with the names of any other assigned custom user roles.

- Step 3** Select the mail policies, content filters, DLP policies, or quarantines for which you want the delegated administrators assigned to be responsible.
 - Step 4** Submit and commit your changes.
-

Editing a Custom User Role

To edit a custom user role, including access privileges:

- Step 1** Go to the **System Administration > User Roles** page.
 - Step 2** Click the user role's name in the Custom User Roles for Delegated Administration listing.
The Edit User Role page appears.
 - Step 3** Make changes to the user role.
 - Step 4** Submit and commit your changes.
-

Duplicating a Custom User Role

You may want to create multiple custom user roles with similar access privileges but assign different responsibilities to different sets of users. For example, if the Email Security appliance handles messages for multiple domains, you may want to create custom user roles with similar access rights but for different mail policies based on the domain. This allows delegated administrators to manage mail policies for their domains without interfering with the responsibilities of other delegated administrators.

To duplicate a custom user role:

- Step 1** Go to the **System Administration > User Roles** page.
 - Step 2** Click the duplicate icon corresponding to the user role you want to duplicate in the Custom User Roles for Delegated Administration listing.
The Add User Role page appears with the access privileges already assigned.
 - Step 3** Change the name of the custom user role.
 - Step 4** Make any access privilege changes required for the new custom user role.
 - Step 5** Submit and commit your changes.
-

Deleting a Custom User Role

When a custom role is deleted, users become unassigned and do not have access to the appliance. You should reassign any users that were assigned to the custom user role that you deleted.

To delete a custom user role:

- Step 1** Go to the **System Administration > User Roles** page.

- Step 2** Click the trash can icon corresponding to the user role you want to delete in the Custom User Roles for Delegated Administration list. The Add User Role page appears.
- Step 3** Confirm the deletion by clicking **Delete** in the warning dialog that appears.
- Step 4** 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 Cisco 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 Cisco IronPort appliance, click the Configuration File link on the System Administration tab.

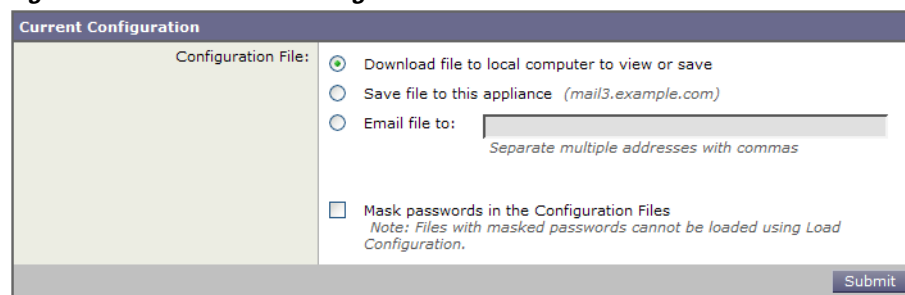
The Configuration File page contains three sections:

- **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 8-24 Current Configuration File



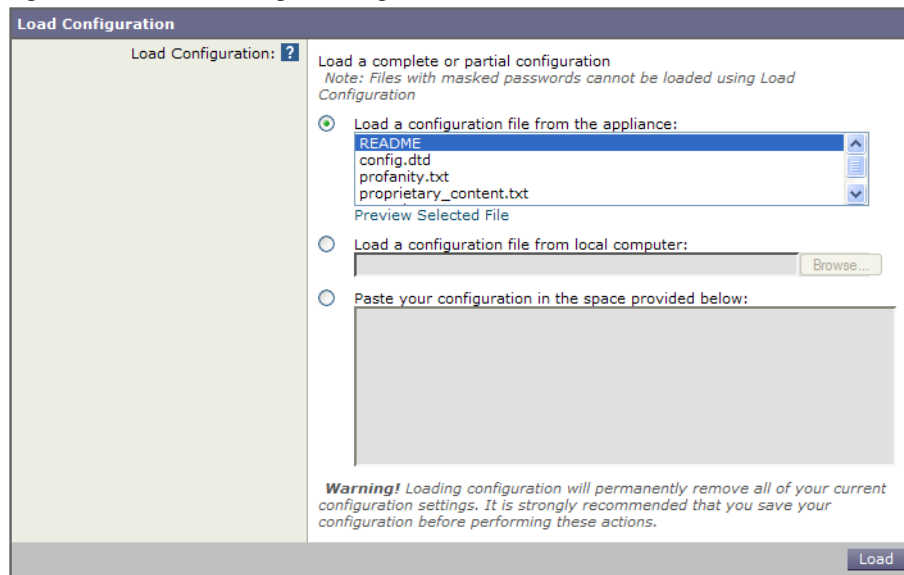
You can mask the user's passwords by clicking the checkbox. Masking a password causes the original, encrypted password to be replaced with "*****" in the exported or saved file. Please note, however, that configuration files with masked passwords cannot be loaded back into AsyncOS.

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 8-25 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 Cisco 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>mail14.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:

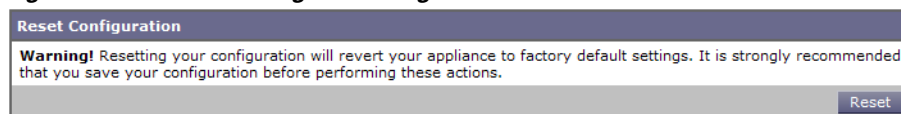
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

Currently, only configuration files with this encoding can be loaded.

Resetting the Current Configuration

Resetting the current configuration causes your Cisco 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 8-26 *Resetting the Configuration File*



See [Resetting to Factory Defaults, page 8-5](#).

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 8-5](#).)

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 8-40](#).



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 on the appliance.

```
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**

File written on machine "mail3.example.com" to the location
"/configuration/C360-420E874BB4B3C41C5C71-1419B58528A0-20120105T214041.xml".
Configuration saved.

```
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 8-37](#) 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 Cisco 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

System status: online

[rest of command deleted]



CHAPTER 9

Testing and Troubleshooting

This chapter contains the following sections:

- [Debugging Mail Flow Using Test Messages: Trace, page 9-1](#)
- [Using the Listener to Test the Appliance, page 9-16](#)
- [Troubleshooting the Network, page 9-20](#)
- [Troubleshooting the Listener, page 9-26](#)
- [Troubleshooting Delivery, page 9-27](#)
- [Troubleshooting Performance, page 9-30](#)

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 Cisco Systems offers Technical Support for complex issues (see [Cisco IronPort Customer Support, page 1-4](#)).



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 <code>trace</code> command prompts for an IP address and a fully-qualified domain name. It does <i>not</i> attempt to reverse the IP address to see if it matches the fully-qualified domain name. The <code>trace</code> 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.	<code>203.45.98.109</code>
Fully Qualified Domain Name of the Source IP	Type the fully-qualified remote domain name to mimic.	<code>smtp.example.com</code>
Listener to Trace Behavior on	Choose from the list of listeners configured on the system to emulate sending the test message to.	<code>InboundMail</code>
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.	<code>34</code>
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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.	<code>-7.5</code>
Envelope Sender	Type the Envelope Sender of the test message.	<code>admin@example.net</code>
Envelope Recipients	Type a list of recipients for the test message. Separate multiple entries with commas.	<code>joe</code> <code>frank@example.com</code>
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.	<code>To: 1@example.com</code> <code>From: ralph</code> <code>Subject: Test</code> <code>this is a test message</code> <code>.</code>

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	<p>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.</p> <p>If the Cisco IronPort appliance was configured to reject the connection (either through a REJECT or TCPREFUSE access rule), the <code>trace</code> command exits at the point in the processing.</p> <p>For more information on setting HAT parameters, see “The Host Access Table (HAT): Sender Groups and Mail Flow Policies” in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>
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 <code>trace</code> command prints “Processing MAIL FROM:” before this section.	
Default Domain	<p>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.</p> <p>For more information, see the “Customizing Listeners” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

Table 9-2 Viewing Output When Performing a Trace (continued)

trace Command Section	Output
Masquerading	<p>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 <code>listenerconfig -> edit -> masquerade -> config</code> subcommands.</p> <p>For more information, see the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
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 <code>trace</code> command prints “Processing Recipient List:” before this section.	
Default Domain	<p>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.</p> <p>For more information, see the “Customizing Listeners” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Domain Map Translation	<p>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.</p> <p>For more information, see the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Recipient Access Table (RAT)	<p>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.)</p> <p>For more information on specifying recipients you accept, see the “Configuring the Gateway to Receive Email” chapter in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>
Alias Table	<p>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.</p> <p>For more information, see the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

Table 9-2 Viewing Output When 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 <code>250 ok</code> command is returned to the remote MTA.	
The <code>trace</code> command prints “Message Processing:” before this section.	
Virtual Gateways	<p>The <code>altsrchost</code> 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 <code>altsrchost</code> command, that information is printed in this section.</p> <p>Note that the virtual gateway address assigned at this point may be overridden by message filter processing below.</p> <p>For more information, see the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Bounce Profiles	<p>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.</p> <p>For more information, see the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>

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 <code>status</code> and <code>status detail</code> commands.	
Masquerading	<p>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 <code>listenerconfig -> edit -> masquerade -> config</code> subcommands.</p> <p>For more information, see the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
LDAP Routing	<p>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.</p> <p>For more information, see the “LDAP Queries” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
Message Filters Processing	<p>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 <code>else</code> clause, those actions are evaluated instead. The results of the message filters, processed in order, are printed in this section.</p> <p>See the “Using Message Filters to Enforce Email Policies” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
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	<p>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 <code>trace</code> command processing stops.</p> <p>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.</p> <p>See the “Anti-Spam” chapter in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.</p>
Anti-Virus	<p>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 <code>trace</code> command processing stops.</p> <p>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.</p> <p>See the “Anti-Virus” chapter in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.</p>
Content Filters Processing	<p>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.</p> <p>See the “Email Security Manager” chapter in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>

Table 9-2 **Viewing Output When Performing a Trace (continued)**

trace Command Section	Output
VOF Processing	<p>This section notes messages that contain attachments are to bypass the Outbreak Filters feature. If messages are to be processed by 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.</p> <p>See the “Outbreak Filters” chapter in the <i>Cisco IronPort AsyncOS for Email Configuration Guide</i> for more information.</p>
Footer Stamping	<p>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 <i>Cisco IronPort AsyncOS for Email Configuration Guide</i>.</p>

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 <code>trace</code> command prints “Message Enqueued for Delivery” before this section.	
Global Unsubscribe per Domain and per User	<p>If any recipients you specified as input for the <code>trace</code> 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.</p> <p>See the “Configuring Routing and Delivery Features” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced Configuration Guide</i>.</p>
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*
Trace

Message Definition	
Sender Information	
Source IP:	<input type="text" value="1.2.3.4"/>
Fully Qualified Domain Name of the Source IP: ?	<input type="text" value="remotehost.example.com"/>
Listener to Trace Behavior on:	<input type="button" value="Public (172.22.85.1:25)"/> ▼
SenderBase Network Owner ID:	<input checked="" type="radio"/> Lookup network owner ID associated with source IP <input type="radio"/> Use: <input type="text"/>
SenderBase Reputation Score (SBRs):	<input checked="" type="radio"/> Lookup SBRs associated with source IP <input type="radio"/> Use: <input type="text"/>
Envelope Information	
Envelope Sender:	<input type="text" value="pretend.sender@example.domain"/>
Envelope Recipients (separated by commas):	<input type="text" value="admin@ironport.com"/>
Message Body	
Upload Message Body:	<input type="text"/> <input type="button" value="Browse..."/>
Paste Message Body: (If no file is uploaded.)	<div>Subject: hello</div> <div>This is a test message.</div>

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		

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:	<p>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"</p> <p>Subject: hello Content-Transfer-Encoding: base64 Content-Type: text/plain; charset="utf-8"</p> <p>VGhpcyBpcyBhIHRlc3QgbWVzc2FnZS4KPT09PT09PT09CuODleODg+OCv+ODv+OObP+OBmeOA guOCj+OBhOOCj+OBhOOAggpUaGlzIGlzIGEgSmFwYW5lc2UgZm9vdGVyCj09PT09PT09PT09PQo=</p>

Done

```
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)
- 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]>
```

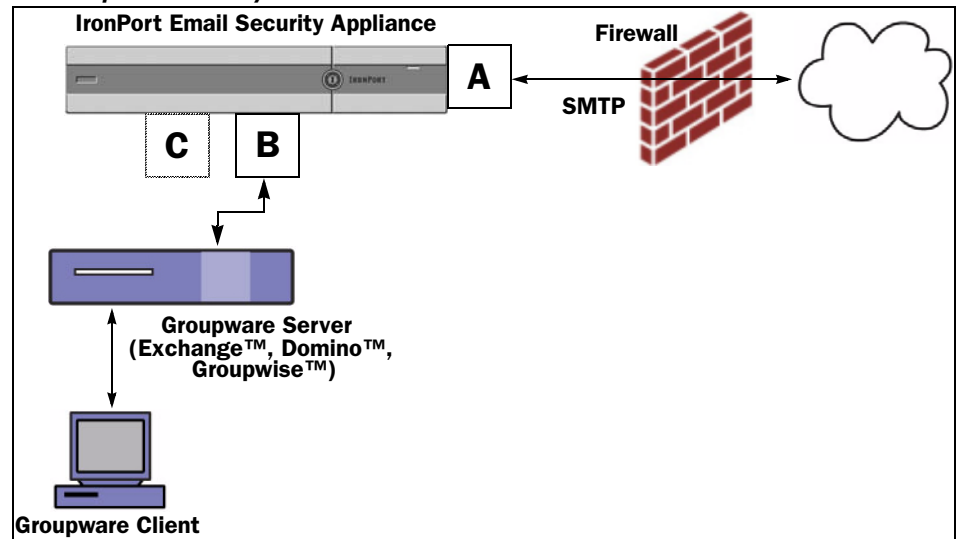
Using the Listener to Test the Appliance

“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 queueing 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 addresses 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 6-6](#)
- [Other Tasks in the GUI, page 7-1](#)

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 6-6.](#))

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 8-8](#).

- 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 -> smtping` 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 6-12.](#))

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. An 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 5-8](#) and [Using IronPort Injection Debug Logs, page 5-23](#).

## 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 is 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 5-22](#).

**Bounce logs** record all information pertaining to each bounced recipient.

For more information, see [Using IronPort Bounce Logs, page 5-17](#).

**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 5-8](#).

- 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]> mx.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 mx.example.com.

TLS certificate match mx.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.

```
TLS successfully connected to mx.example.com.
```

```
TLS verification completed.
```

## Troubleshooting Performance

If you suspect that 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 [Displaying Real-time Activity, page 6-17](#).

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 Cisco IronPort Customer Support. See [Cisco IronPort Customer Support, page 1-4](#).

- 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 6-24](#). Use these commands:

- `deleterecipients`
- `bouncerecipients`

- `redirectrecipients`
- `suspenddel / resumedel`
- `suspendlistener / resumelister`

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.





## INDEX

---

### A

accessing [2-2](#)  
access privileges for custom user roles [8-28](#)  
Account Privileges page [8-27](#)  
Anti-Spam Archive Logs [5-3](#)  
Anti-spam logs [5-3](#)  
Anti-Virus Archive Logs [5-3](#)  
Anti-Virus Logs [5-3](#)  
archivemessage command [6-37](#)  
archiving reports [2-43](#)

---

### B

blackhole listener [9-16](#)  
Bounce Logs [5-2](#)  
bouncerecipients command [6-26](#)  
bouncing recipients  
    all [6-28](#)  
    by Envelope From [6-28](#)  
    by hostname [6-28](#)

---

### C

Change Password link [8-18](#)  
changing your password [8-18](#)  
clean message [2-7](#)  
CLI Audit Logs [5-3](#)  
Cloud user types [8-26](#)  
community string [6-40](#)  
configuration file [8-36](#)  
    CLI [8-41](#)  
    GUI [8-36](#)

XML [8-36](#)

connectivity issues, troubleshooting [9-20](#)  
counters [6-1](#)  
CPU usage [6-4](#)  
CSV data [2-42](#)  
custom user roles [8-26](#)

---

### D

daily magnitude [2-12](#)  
Default Action  
    delete [4-5](#)  
    for quarantine [4-4](#)  
    release [4-5](#)  
delegated administration [8-26](#)  
delete all messages in the IronPort Spam quarantine [4-37](#)  
deleterecipients command [6-24](#)  
delivernow command [6-34](#)  
Delivery Connection ID (DCID) [6-4](#)  
Delivery Logs [5-2](#)  
delivery queue [6-24](#)  
delivery queue, monitoring [6-16](#)  
Delivery Status Details page [2-20](#)  
Delivery Status page [2-19](#)  
diagnostic -> network -> arpshow command [9-22](#)  
diagnostic -> network -> flush command [9-22](#)  
diagnostic -> network -> smtppping command [9-23](#)  
DNS  
    A Record [9-26](#)  
    cache [9-25](#)  
    double lookup [2-10](#)  
    PTR record [9-26](#)  
    testing [9-24](#)

DNS cache [6-22](#)  
 DNS lookup [6-22](#)  
 dnsstatus command [6-22](#)  
 Domain Debug Logs [5-2](#)  
 domains [2-13](#)  
 double-DNS verified [2-11](#)  
 DTD (document type definition) [8-38](#)

---

## E

Early Expiration  
     for quarantine [4-5](#)  
 email  
     clean message [2-7](#)  
 Email Security Monitor [2-1, 2-2](#)  
     automated reporting [2-42](#)  
     external domains received listing [2-10](#)  
     Items Displayed menu [2-11](#)  
     mail trend graph [2-5](#)  
     summary table [2-6](#)  
     Time Range menu [2-5](#)  
 Envelope Recipient [3-4](#)  
 Envelope Sender [3-4](#)  
 event tracking [3-5](#)  
     Currently in Outbreak Quarantine [3-5](#)  
     Delivered [3-5](#)  
     DLP Violations [3-5](#)  
     Hard Bounced [3-5](#)  
     Quarantined as Spam [3-5](#)  
     Soft Bounced [3-5](#)  
     Spam Positive [3-5](#)  
     Suspect Spam [3-5](#)  
     Virus Positive [3-5](#)  
 external authentication  
     enabling LDAP [8-24](#)  
     enabling RADIUS [8-25](#)

---

## F

feature key [8-11](#)  
 feature keys  
     adding (GUI) manually [8-12](#)  
 findevent [6-38](#)  
 firewall permissions [9-26](#)  
 forward DNS lookup [6-21](#)  
 FTP Push [5-6](#)  
 FTP Server Logs [5-3](#)

---

## G

gauges [6-1, 6-4](#)  
 global counters [6-23](#)  
 graph [2-4](#)  
 graphical user interface  
     see *GUI*  
 graphs [7-5](#)  
 GUI  
     enabling [7-1](#)  
     overview [7-1](#)

---

## H

hostrate command [6-19](#)  
 hoststatus command [2-20, 6-14](#)  
 HTTP  
     GUI [7-1](#)  
 HTTP authentication [2-42](#)  
 HTTP Logs [5-3](#)  
 HTTPS  
     GUI [7-1](#)

---

## I

IMAP authentication [4-24](#)  
 Incoming Mail Reporting page [2-7](#)

Injection Connection ID (ICID) [6-4](#)

Injection Debug Logs [5-2](#)

international character sets [3-4](#)

invalid recipient [2-6](#)

IP addresses [2-13](#)

IP address profile pages [2-12](#)

IPMI [6-40](#)

IronPort Spam Quarantine

behavior when full [4-22](#)

configuring [4-18](#)

default language [4-23](#)

defined [4-1](#)

deleting all messages [4-19, 4-37](#)

disabling [4-19](#)

end user access without authentication [4-24](#)

end user authentication [4-24](#)

IMAP/POP authentication [4-32](#)

LDAP authentication [4-31](#)

message details [4-36](#)

message variables [4-26](#)

notification [4-2](#)

priority [4-18](#)

receiving multiple notifications [4-33](#)

released messages and email pipeline [4-36](#)

testing notifications [4-32](#)

IronPort Text Mail Logs [5-2](#)

---

## K

keys [8-11](#)

---

## L

language

specifying a default language for IronPort Spam Quarantine [4-23](#)

last command [8-19](#)

LDAP

external authentication [8-24](#)

LDAP Debug Logs [5-3](#)

load [6-4](#)

loadconfig command [8-42](#)

log file type [5-2](#)

logging

overview [5-1](#)

logheaders command [5-43](#)

logs

Anti-Spam Archive [5-3](#)

Anti-Virus [5-3](#)

Anti-Virus Archive [5-3](#)

Bounce Logs [5-2](#)

CLI Audit Logs [5-3](#)

comparison [5-4](#)

Configuration History Logs [5-37](#)

definition [5-1](#)

Delivery Logs [5-2](#)

extensions in filenames [5-44](#)

format [5-1](#)

FTP Server Logs [5-3](#)

global attributes [5-42](#)

HTTP Logs [5-3](#)

Injection Debug Logs [5-2](#)

IronPort Text Mail Logs [5-2](#)

LDAP Debug Logs [5-3](#)

levels [5-39](#)

log subscription defined [5-1](#)

message headers in [5-43](#)

NTP Logs [5-3](#)

qmail Format Delivery Logs [5-2](#)

rolling over [5-6](#)

Scanning [5-3](#)

SCP Push [5-6](#)

Status Logs [5-2](#)

subscriptions [5-6](#)

syslog push [5-6](#)

troubleshooting with [9-27](#)

log subscription [5-1](#)

log subscriptions [5-6](#)

---

**M**

[mailconfig command](#) [8-41](#)  
[mailing lists](#)  
     [notifications](#) [4-21](#)  
[mail trend graph](#) [2-4](#)  
[matched content](#) [4-10](#)  
[memory](#) [6-5](#)  
[message headers](#) [5-43](#)  
[Message ID \(MID\)](#) [6-3](#)  
[message tracking](#)  
     <emphasis>See [tracking](#)  
[message variables](#)  
     [IronPort Spam quarantine notifications](#) [4-26](#)  
[MIB file](#) [6-40](#)  
[monitoring](#) [6-1, 6-7](#)  
[MX records](#) [9-26](#)

---

**N**

[netstat command](#) [9-22](#)  
[network owner](#) [2-13](#)  
[Network Owner profile pages](#) [2-12](#)  
[network problems, troubleshooting](#) [9-22](#)  
[non-ascii character sets](#) [3-4](#)  
[Normal Expiration](#)  
     [for quarantine](#) [4-4](#)  
[No Subject](#) [3-7](#)  
[nslookup command](#) [9-24](#)  
[NTP Logs](#) [5-3](#)

---

**O**

[offline command](#) [8-2](#)  
[offline state](#) [8-2](#)  
[oldmessage command](#) [6-37](#)  
[opening links in a separate window](#) [2-5](#)  
[Outgoing Destinations page](#) [2-17](#)  
[Outgoing Senders page](#) [2-18](#)

[Overview page \(Security Monitor\)](#) [2-4](#)

---

**P**

[packet capture](#) [8-8](#)  
[password](#)  
     [changing](#) [8-18](#)  
     [settings](#) [8-20](#)  
[pausing the work queue](#) [6-35](#)  
[performance](#) [9-30](#)  
[ping command](#) [9-22](#)  
[POP authentication](#) [4-24](#)  
[power down](#) [8-2](#)  
[present in the Local Quarantines listing](#) [4-3](#)  
[Profile for Domain pages](#) [2-12](#)

---

**Q**

[qmail Format Delivery Logs](#) [5-2](#)  
[quarantine](#) [4-1](#)  
     ["AND" searches](#) [4-14](#)  
     [adding X-Headers](#) [4-5](#)  
     [allocating space for](#) [4-4](#)  
     [applying actions to messages in](#) [4-10](#)  
     [default action](#) [4-4](#)  
     [delay exit](#) [4-4](#)  
     [displaying non-ascii characters in subject](#) [4-5](#)  
     [early expiration](#) [4-5](#)  
     [In other quarantines](#) [4-9](#)  
     [international character sets](#) [4-10](#)  
     [minimum size](#) [4-4](#)  
     [multiple IronPort Spam quarantines](#) [4-18](#)  
     [normal expiration](#) [4-4](#)  
     [Outbreak quarantine special filters](#) [4-17](#)  
     [reporting messages to IronPort](#) [4-17](#)  
     [retention time](#) [4-4](#)  
     [setup workflow](#) [4-6](#)  
     [stripping attachments](#) [4-5](#)



- subject tagging [4-5](#)
- testing messages for viruses [4-13](#)
- quarantines
  - overflow message handling [4-5](#)

## R

- RADIUS external authentication [8-25](#)
- RAM [9-30](#)
- RAM Utilization [6-4](#)
- rate command [6-19](#)
- rates [6-1, 6-6](#)
- real-time monitoring [6-17](#)
- reboot command [8-2](#)
- receiving errors [9-27](#)
- redirectrecipients [6-28](#)
- removemessage command [6-37](#)
- reports
  - archiving [2-43](#)
- resetconfig command [8-5](#)
- resetcounters command [2-40, 6-23](#)
- resetting [8-5](#)
- Resource Conservation mode [6-4, 9-30](#)
- resume command [6-34, 8-4](#)
- resumedel command [6-32](#)
- resumelistener command [6-33](#)
- resuming email delivery [6-32](#)
- resuming receiving [6-33](#)
- Retention Time
  - for quarantine [4-4](#)
- retry message delivery [2-20](#)
- reverse DNS [3-8](#)
- reverse DNS lookup [6-21](#)
- RFC
  - 1065 [6-39](#)
  - 1066 [6-39](#)
  - 1067 [6-39](#)
  - 1213 [6-39](#)
  - 1907 [6-39](#)

- 2047 [4-5](#)
- 2571-2575 [6-39](#)
- rolling over log files [5-44](#)
- rollovernow command [5-6](#)

## S

- saveconfig command [8-42](#)
- SBRS score [3-8](#)
- Scanning Logs [5-3](#)
- scheduled log rollover [5-45](#)
- SCP Push [5-6](#)
- SenderBase Reputation Score [7-7, 9-2](#)
- SenderBase reputation score [3-8](#)
- SenderBase Reputation Service [2-1, 2-12](#)
- separate window icon [2-5](#)
- showconfig command [8-41](#)
- showmessage command [6-37](#)
- showrecipients [6-29](#)
- shutdown command [8-1](#)
- shutting down [8-2](#)
- SMI file [6-40](#)
- SMTP Authentication [3-7](#)
- SMTP HELO command [9-26](#)
- SNMP
  - community string [6-40](#)
  - hardware failure trap conditions [6-41](#)
  - IPMI [6-40](#)
  - MIB file [6-40](#)
  - overview [6-39](#)
  - SMI file [6-40](#)
  - specifying multiple trap targets [6-42](#)
  - traps [6-42](#)
- SNMP (Simple Network Management Protocol) [6-39](#)
- SNMPv1 [6-40](#)
- SNMPv2 [6-40](#)
- SNMPv3 passphrase [6-39](#)
- spam message [2-6](#)
- SSH1

- disabling [8-45](#)
- sshconfig command [8-44](#)
- SSH protocol [8-44](#)
  - disabling SSH1 [8-45](#)
- stateless logs [5-15](#)
- status command [6-8](#)
- status detail command [6-9](#)
- Status Logs [5-2](#)
- stopped by content filter [2-7](#)
- stopped by reputation filtering [2-6](#)
- subject
  - no subject [3-7](#)
- supportrequest command [8-7](#)
- suspend command [8-2](#)
- suspenddel command [6-31](#)
- suspending email delivery [6-31](#)
- suspending receiving [6-32](#)
- suspendlistener command [6-33](#)
- Syslog [5-6](#)
- System Capacity
  - All page [2-38](#)
  - Incoming Mail page [2-34](#)
  - memory page swapping [2-37](#)
  - Outgoing Mail page [2-35](#)
  - System Load page [2-36](#)
  - WorkQueue page [2-33](#)
- System Capacity page [2-32](#)
- System Logs [5-2](#)
- system monitoring through the GUI [7-1](#)
- system quarantine [4-3](#)
- System Status page [2-38](#)

---

## T

- tail command [5-47](#)
  - parameters [5-48](#)
- Threat Operations Center (TOC) [2-4](#)
- tlsverify command [9-29](#)
- tophosts command [6-17, 9-24](#)

- topin command [6-21](#)
- trace command [7-6, 9-1](#)
- Trace page [7-6, 9-1](#)
- tracking
  - "AND" searches [3-5](#)
  - advanced options [3-3](#)
  - event [3-5](#)
  - message details [3-3](#)
  - result set, narrowing [3-6](#)
- troubleshooting [9-1](#)
- troubleshooting delivery [9-27](#)
- TTL [6-13](#)
- turning off [8-2](#)

---

## U

- user accounts [8-12](#)
  - limits [8-13](#)
  - locking and unlocking [8-16](#)
- user groups [8-13](#)
- user name [8-16](#)
- user password length [8-16](#)
- user types [8-13](#)
- UTF-8 [3-4](#)

---

## V

- version [2-39](#)
- viewing matched content [4-10](#)
- viewing messages in the system quarantine [4-10](#)
- virus message [2-6](#)
- Virus Types page [2-28](#)

---

## W

- whoami command [8-19](#)
- who command [8-19](#)
- work queue [6-5, 6-35](#)

work queue, pausing [6-35](#)

---

## X

XML [5-2](#), [7-16](#), [8-36](#), [8-38](#), [8-41](#)

XML Status feature [7-16](#)

