



# **Cisco IronPort AsyncOS 7.7 for Security Management User Guide**

July 12, 2011

## **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-23827-01

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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 7.7 for Security Management User Guide*

© 2008-2011 Cisco Systems, Inc. All rights reserved.



# CONTENTS

---

## CHAPTER 1

### **Getting Started with the Security Management Appliance 1-1**

Security Management Appliance Overview 1-1

Supported Services on the Security Management Appliance 1-3

Email Security Management 1-3

Web Security Management 1-4

Additional Features 1-4

What's New in This Release 1-5

How to Use This Guide 1-8

Before You Begin 1-8

Email Security Appliances 1-9

Web Security Appliances 1-9

Security Management Appliances 1-10

Document Conventions 1-10

Where to Find More Information 1-11

Documentation Set 1-11

Cisco IronPort Technical Training 1-12

Knowledge Base 1-13

Cisco Support Community 1-14

Cisco IronPort Customer Support 1-14

Third Party Contributors 1-14

Cisco IronPort Welcomes Your Comments 1-15

**CHAPTER 2**

**Setup and Installation 2-1**

Installation Planning 2-2

Mail Flow When Using the Security Management Appliance as an External Spam Quarantine 2-3

Centralized Management and the Security Management Appliance 2-4

Physical Dimensions 2-4

Preparing for Setup 2-5

Understanding the System Setup Steps 2-6

Determining Network and IP Address Assignments 2-6

Gathering the Setup Information 2-7

Accessing the Graphical User Interface 2-8

Accessing the Web Interfaces of the Security Management Appliance 2-8

Accessing the Security Management Appliance Command Line Interface 2-9

Understanding the System Setup Wizard 2-9

Browser Requirements 2-10

Support Languages 2-11

Running the System Setup Wizard 2-11

Step 1: Review the End User License Agreement 2-12

Step 2: Configure the System Settings 2-13

Step 3: Configure the Network Settings 2-14

Step 4: Review Your Configuration 2-16

Proceeding to the Next Steps 2-17

Security Management Appliance User Interface 2-17

Tabs on the System Status Page 2-19

Commit Changes Button 2-20

Accessing Customer Support from the Security Management Appliance 2-20

Technical Support 2-21

Support Request 2-21

|                                 |      |
|---------------------------------|------|
| Remote Access                   | 2-23 |
| Packet Capture                  | 2-24 |
| Starting a Packet Capture       | 2-25 |
| Editing Packet Capture Settings | 2-27 |
| Working with Feature Keys       | 2-30 |
| Feature Keys Page               | 2-30 |
| Feature Key Settings Page       | 2-31 |
| Expired Feature Keys            | 2-32 |
| SMA Compatibility Matrix        | 2-32 |

---

**CHAPTER 3****Appliance Configuration 3-1**

|                                                                                                 |      |
|-------------------------------------------------------------------------------------------------|------|
| Appliance Configuration Overview                                                                | 3-1  |
| Enabling Services on the Security Management Appliance                                          | 3-2  |
| Enabling and Disabling Centralized Email Reporting on a Security Management Appliance           | 3-3  |
| Disabling Centralized Email Reporting                                                           | 3-4  |
| Enabling and Disabling Centralized Web Reporting on a Security Management Appliance             | 3-5  |
| Disabling Centralized Web Reporting                                                             | 3-6  |
| Enabling and Disabling Centralized Email Tracking on a Security Management Appliance            | 3-6  |
| Disabling Centralized Email Tracking                                                            | 3-7  |
| Enabling and Disabling the Cisco IronPort Spam Quarantine on a Security Management Appliance    | 3-8  |
| Disabling the Cisco IronPort Spam Quarantine                                                    | 3-9  |
| Enabling and Disabling the Centralized Configuration Manager on a Security Management Appliance | 3-9  |
| Disabling the Cisco IronPort Centralized Configuration Manager                                  | 3-10 |
| Adding Managed Appliances                                                                       | 3-10 |
| Editing and Deleting Managed Appliances                                                         | 3-14 |

|                                                        |      |
|--------------------------------------------------------|------|
| Editing a Managed Appliance                            | 3-14 |
| Deleting a Managed Appliance                           | 3-15 |
| About Reports                                          | 3-16 |
| Reporting Options                                      | 3-16 |
| How the Security Appliance Gathers Data for Reports    | 3-16 |
| How Reporting Data is Stored                           | 3-17 |
| Interactive Report Pages                               | 3-17 |
| Choosing a Time Range for Interactive Reports          | 3-18 |
| Reporting Filters on the Security Management Appliance | 3-19 |
| Printing and Exporting Report Data                     | 3-20 |
| Exporting Report Data                                  | 3-21 |

## CHAPTER 4

### Using Centralized Email Reporting 4-1

|                                                      |      |
|------------------------------------------------------|------|
| Reporting Overview                                   | 4-1  |
| Getting Started with Email Reporting                 | 4-2  |
| Configuring Centralized Email Reporting              | 4-2  |
| Creating Email Reporting Groups                      | 4-4  |
| Adding Email Reporting Groups                        | 4-5  |
| Editing and Deleting Email Reporting Groups          | 4-6  |
| Using the Email Reporting Tab                        | 4-6  |
| Viewing Interactive Reports                          | 4-9  |
| Searching and the Interactive Report Pages           | 4-10 |
| Reporting Filters for Report Pages                   | 4-11 |
| Printing and Exporting Reports from Report Pages     | 4-11 |
| More Information about Reports and Report Pages      | 4-11 |
| Understanding the Email Reporting Pages              | 4-11 |
| Email Reporting Overview Page                        | 4-12 |
| How Incoming Mail Messages are Counted               | 4-15 |
| How Email Messages Are Categorized by the Appliances | 4-15 |

|                                                           |      |
|-----------------------------------------------------------|------|
| Categorizing Email Messages on Overview Page              | 4-16 |
| Incoming Mail Page                                        | 4-17 |
| Views Within the Incoming Mail Page                       | 4-18 |
| Categorizing Email Messages on Incoming Mail Page         | 4-20 |
| Incoming Mail Details Table                               | 4-24 |
| Sender Profile Pages                                      | 4-25 |
| Sender Groups Report Page                                 | 4-30 |
| Outgoing Destinations Page                                | 4-31 |
| Outgoing Senders Page                                     | 4-33 |
| Internal Users Page                                       | 4-36 |
| Internal User Details Page                                | 4-38 |
| Searching for a Specific Internal User                    | 4-39 |
| DLP Incident Summary Page                                 | 4-40 |
| DLP Incidents Details Table                               | 4-42 |
| DLP Policy Detail Page                                    | 4-43 |
| Content Filters Page                                      | 4-43 |
| Content Filter Details Page                               | 4-45 |
| Virus Types Page                                          | 4-45 |
| TLS Connections Page                                      | 4-48 |
| Outbreak Filters Page                                     | 4-51 |
| System Capacity Page                                      | 4-55 |
| How to Interpret the Data You See on System Capacity Page | 4-56 |
| System Capacity – Workqueue                               | 4-56 |
| System Capacity – Incoming Mail                           | 4-57 |
| System Capacity – Outgoing Mail                           | 4-60 |
| System Capacity – System Load                             | 4-62 |
| Note About Memory Page Swapping                           | 4-63 |
| System Capacity – All                                     | 4-64 |
| Data Availability Page                                    | 4-64 |
| About Scheduled and On-Demand Reports                     | 4-66 |

|                                       |      |
|---------------------------------------|------|
| Additional Report Types               | 4-68 |
| Domain-Based Executive Summary Report | 4-68 |
| Executive Summary Reports             | 4-73 |
| Generating Reports On Demand          | 4-73 |
| Scheduled Reports                     | 4-75 |
| Adding Scheduled Reports              | 4-76 |
| Editing Scheduled Reports             | 4-77 |
| Discontinuing Scheduled Reports       | 4-78 |
| Archived Reports                      | 4-78 |
| Accessing Archived Reports            | 4-79 |
| Deleting Archived Reports             | 4-80 |

## CHAPTER 5

### Using Centralized Web Reporting 5-1

|                                                                         |      |
|-------------------------------------------------------------------------|------|
| Reporting Overview                                                      | 5-1  |
| Getting Started with Web Reporting                                      | 5-3  |
| Configuring Centralized Web Reporting                                   | 5-3  |
| Using the Web Reporting Tab                                             | 5-5  |
| Interactive Report Pages for the Web Security Appliance                 | 5-10 |
| Configuring Column Settings on Report Pages                             | 5-10 |
| Printing Reports from Report Pages                                      | 5-11 |
| Reporting Filters for Report Pages                                      | 5-11 |
| Understanding the Web Reporting Pages                                   | 5-11 |
| Web Reporting Overview Page                                             | 5-12 |
| Users Page                                                              | 5-16 |
| User Details Page                                                       | 5-20 |
| Web Sites Page                                                          | 5-24 |
| URL Categories Page                                                     | 5-28 |
| Using The URL Categories Page in Conjunction with Other Reporting Pages | 5-32 |



|                                                                           |      |
|---------------------------------------------------------------------------|------|
| Custom URL Categories                                                     | 5-33 |
| Reporting Misclassified and Uncategorized URLs                            | 5-35 |
| Application Visibility Page                                               | 5-36 |
| Understanding the Difference between Application versus Application Types | 5-36 |
| Anti-Malware Page                                                         | 5-41 |
| Malware Category Report Page                                              | 5-42 |
| Malware Threat Report Page                                                | 5-43 |
| Malware Category Descriptions                                             | 5-45 |
| Configuring Anti-Malware                                                  | 5-46 |
| Client Malware Risk Page                                                  | 5-50 |
| Client Detail Page                                                        | 5-53 |
| Web Reputation Filters Page                                               | 5-57 |
| What are Web Reputation Filters?                                          | 5-57 |
| Configuring Web Reputation Scores                                         | 5-61 |
| Configuring Web Reputation Filter Settings for Access Policies            | 5-61 |
| L4 Traffic Monitor Data Page                                              | 5-63 |
| Configuring the L4 Traffic Monitor                                        | 5-65 |
| Reports by User Location Page                                             | 5-66 |
| Web Tracking Page                                                         | 5-69 |
| Configuring Web Tracking                                                  | 5-71 |
| Default Web Tracking Results                                              | 5-71 |
| Advanced Web Tracking Results                                             | 5-73 |
| System Capacity Page                                                      | 5-74 |
| How to Interpret the Data You See on System Capacity Page                 | 5-75 |
| System Capacity—System Load                                               | 5-76 |
| System Capacity—Network Load                                              | 5-78 |
| Data Availability Page                                                    | 5-80 |
| Scheduling Reports                                                        | 5-82 |

|                                |      |
|--------------------------------|------|
| Managing Scheduled Reports     | 5-83 |
| Adding Scheduled Reports       | 5-83 |
| Editing Scheduled Reports      | 5-85 |
| Deleting Scheduled Reports     | 5-85 |
| Additional Extended Reports    | 5-85 |
| Top URL Categories—Extended    | 5-85 |
| Top Application Types—Extended | 5-87 |
| Archiving Reports              | 5-89 |
| ‘Generate Report Now’ Option   | 5-89 |

## CHAPTER 6

### Tracking Email Messages 6-1

|                                               |      |
|-----------------------------------------------|------|
| Tracking Service Overview                     | 6-1  |
| About Setting Up Centralized Message Tracking | 6-3  |
| Understanding Tracking Query Setup            | 6-3  |
| Running a Search Query                        | 6-7  |
| Narrowing the Result Set                      | 6-8  |
| Understanding Tracking Query Results          | 6-9  |
| Message Details                               | 6-10 |

## CHAPTER 7

### Managing the Cisco IronPort Spam Quarantine 7-1

|                                                                     |      |
|---------------------------------------------------------------------|------|
| Understanding the Cisco IronPort Spam Quarantine                    | 7-1  |
| Configuring Cisco IronPort Spam Quarantine Settings                 | 7-3  |
| Configuring Administrative Users for Cisco IronPort Spam Quarantine | 7-6  |
| Configuring End User Access and Notifications                       | 7-7  |
| Configuring End User Quarantine Access                              | 7-8  |
| Enabling Spam Notifications                                         | 7-9  |
| Setting Up Email Security Appliances to Forward Spam                | 7-12 |
| Configuring External Quarantine Settings                            | 7-13 |

|                                                                             |      |
|-----------------------------------------------------------------------------|------|
| Adding and Updating Managed Appliances and Using the Quarantine Spam Option | 7-14 |
| Managing Messages in the Cisco IronPort Spam Quarantine                     | 7-15 |
| Searching for Messages in the Cisco IronPort Spam Quarantine                | 7-16 |
| Searching Large Message Collections                                         | 7-17 |
| Viewing Messages in the Cisco IronPort Spam Quarantine                      | 7-17 |
| Viewing HTML Messages                                                       | 7-18 |
| Viewing Encoded Messages                                                    | 7-18 |
| Delivering Messages in the Cisco IronPort Spam Quarantine                   | 7-18 |
| Deleting Messages from the Cisco IronPort Spam Quarantine                   | 7-18 |
| Enabling the End User Safelist/Blocklist Feature                            | 7-19 |
| Enabling and Configuring Safelist/Blocklist Settings                        | 7-20 |
| Backing Up and Restoring the Safelist/Blocklist Database                    | 7-21 |
| Synchronizing Safelist and Blocklist Settings and Databases                 | 7-22 |
| Message Delivery for Safelists and Blocklists                               | 7-22 |
| Troubleshooting Safelists and Blocklists                                    | 7-23 |
| Using End User Safelists and Blocklists                                     | 7-23 |
| Accessing Safelists and Blocklists                                          | 7-24 |
| Adding Entries to Safelists and Blocklists                                  | 7-24 |
| Working with Safelists                                                      | 7-25 |
| Working with Blocklists                                                     | 7-26 |

---

**CHAPTER 8**
**Managing Web Security Appliances 8-1**

|                                                              |     |
|--------------------------------------------------------------|-----|
| Overview of Managing Web Security Appliances                 | 8-1 |
| Working with Configuration Masters                           | 8-3 |
| Important Notes About Using Configuration Masters            | 8-3 |
| Editing Security Services Settings                           | 8-3 |
| Initializing Configuration Masters                           | 8-7 |
| Associating Web Security Appliances to Configuration Masters | 8-8 |
| Configuring Configuration Masters                            | 8-9 |

Populating a Configuration Master with Existing Web Security Appliance Settings 8-10

About Configuring Web Security Features Using Configuration Masters 8-11

Publishing Configurations to Web Security Appliances 8-13

Publishing a Configuration Master 8-15

Using Advanced File Publishing 8-18

Viewing Publish History 8-21

Viewing Web Security Appliance Status 8-22

## CHAPTER 9

### Monitoring System Status 9-1

Monitoring Security Management Appliance Status 9-1

Centralized Services 9-3

Security Appliance Data Transfer Status 9-5

System Information 9-7

Viewing the Status of Your Managed Appliances 9-8

Monitoring Reporting Data Availability Status 9-9

Monitoring Data Availability on your Email Security Appliances 9-9

Monitoring Data Availability on your Web Security Appliances 9-11

Monitoring Tracking Data Status 9-12

Monitoring Email Tracking Data Status 9-12

Monitoring Web Tracking Data Status 9-13

## CHAPTER 10

### LDAP Queries 10-1

Overview 10-1

Configuring LDAP to Work with the Cisco IronPort Spam Quarantine 10-2

Creating the LDAP Server Profile 10-3

Testing LDAP Servers 10-6

Configuring LDAP Queries 10-6

|                                                             |       |
|-------------------------------------------------------------|-------|
| LDAP Query Syntax                                           | 10-6  |
| Tokens                                                      | 10-7  |
| Spam Quarantine End-User Authentication Queries             | 10-8  |
| Sample Active Directory End-User Authentication Settings    | 10-8  |
| Sample OpenLDAP End-User Authentication Settings            | 10-9  |
| Spam Quarantine Alias Consolidation Queries                 | 10-9  |
| Sample Active Directory Alias Consolidation Settings        | 10-10 |
| Sample OpenLDAP Alias Consolidation Settings                | 10-11 |
| Testing LDAP Queries                                        | 10-11 |
| Domain-Based Queries                                        | 10-12 |
| Creating a Domain-Based Query                               | 10-13 |
| Chain Queries                                               | 10-14 |
| Creating a Chain Query                                      | 10-15 |
| Configuring AsyncOS to Work With Multiple LDAP Servers      | 10-16 |
| Testing Servers and Queries                                 | 10-17 |
| Failover                                                    | 10-17 |
| Configuring the Cisco IronPort Appliance for LDAP Failover  | 10-17 |
| Load Balancing                                              | 10-19 |
| Configuring the Cisco IronPort Appliance for Load Balancing | 10-19 |
| Configuring External Authentication for Users               | 10-20 |
| User Accounts Query                                         | 10-21 |
| Group Membership Queries                                    | 10-22 |

## CHAPTER 11

### Configuring SMTP Routing 11-1

|                                 |      |
|---------------------------------|------|
| Routing Email for Local Domains | 11-1 |
| SMTP Routes Overview            | 11-2 |
| Default SMTP Route              | 11-3 |
| Defining an SMTP Route          | 11-3 |
| SMTP Routes Limits              | 11-4 |

|                                                           |      |
|-----------------------------------------------------------|------|
| SMTP Routes and DNS                                       | 11-4 |
| SMTP Routes and Alerts                                    | 11-4 |
| SMTP Routes, Mail Delivery, and Message Splintering       | 11-4 |
| SMTP Routes and Outbound SMTP Authentication              | 11-5 |
| Managing SMTP Routes on the Security Management Appliance | 11-5 |
| Adding SMTP Routes                                        | 11-6 |
| Editing SMTP Routes                                       | 11-6 |
| Deleting SMTP Routes                                      | 11-7 |
| Exporting SMTP Routes                                     | 11-7 |
| Importing SMTP Routes                                     | 11-8 |

## CHAPTER 12

### Common Administrative Tasks 12-1

|                                                                    |       |
|--------------------------------------------------------------------|-------|
| Performing Maintenance Tasks Using CLI Commands                    | 12-2  |
| Shutting Down the Security Management Appliance                    | 12-2  |
| Rebooting the Security Management Appliance                        | 12-3  |
| Placing the Security Management Appliance into a Maintenance State | 12-3  |
| The suspend and offline Commands                                   | 12-5  |
| Resuming from an Offline State                                     | 12-5  |
| The resume Command                                                 | 12-6  |
| Resetting to Factory Defaults                                      | 12-6  |
| The resetconfig Command                                            | 12-7  |
| Displaying the Version Information for AsyncOS                     | 12-8  |
| Backing Up Your Security Management Appliance                      | 12-8  |
| About Backing Up Your Data                                         | 12-8  |
| Restrictions for Backups                                           | 12-9  |
| Backup Duration                                                    | 12-10 |
| Availability of Services During Backups                            | 12-10 |
| Interruption of a Backup Process                                   | 12-11 |
| Scheduling a Backup                                                | 12-11 |
| Periodic Backups                                                   | 12-12 |

|                                                             |       |
|-------------------------------------------------------------|-------|
| Immediate Backups                                           | 12-14 |
| Other Important Backup Tasks                                | 12-15 |
| Upgrading to New Security Management Appliance Hardware     | 12-15 |
| Upgrading AsyncOS                                           | 12-17 |
| Before You Upgrade: Important Steps                         | 12-17 |
| Remote vs. Streaming Upgrades                               | 12-18 |
| Upgrading Clustered Systems                                 | 12-19 |
| Streaming Upgrade Overview                                  | 12-19 |
| Remote Upgrade Overview                                     | 12-20 |
| Hardware and Software Requirements for Remote Upgrades      | 12-21 |
| Hosting a Remote Upgrade Image                              | 12-22 |
| Obtaining Upgrades Using the GUI                            | 12-22 |
| Upgrading AsyncOS from the GUI                              | 12-23 |
| Reverting to an Earlier Version of AsyncOS                  | 12-25 |
| Important Note About Reversion Impact                       | 12-25 |
| Performing the AsyncOS Reversion                            | 12-25 |
| Obtaining Upgrades Using the CLI                            | 12-29 |
| The updateconfig Command                                    | 12-29 |
| The upgrade Command                                         | 12-30 |
| Differences Between Upgrading Methods (Remote vs Streaming) | 12-31 |
| Configuring Upgrade and Service Update Settings             | 12-32 |
| Editing Update Settings                                     | 12-32 |
| Configuring the Update and Upgrade Settings from the GUI    | 12-34 |
| Disaster Recovery on the Security Management Appliance      | 12-36 |
| About Distributing Administrative Tasks                     | 12-40 |
| User Roles                                                  | 12-40 |
| Delegating Administration with Custom User Roles            | 12-45 |
| About Custom Email User Roles                               | 12-45 |
| Creating Custom Email User Roles                            | 12-48 |
| Editing Custom Email User Roles                             | 12-50 |

|                                                                      |       |
|----------------------------------------------------------------------|-------|
| Using Custom Email User Roles                                        | 12-50 |
| About Custom Web User Roles                                          | 12-51 |
| Creating Custom Web User Roles                                       | 12-52 |
| Editing Custom Web User Roles                                        | 12-54 |
| Managing Users with the GUI                                          | 12-55 |
| Adding Users                                                         | 12-57 |
| Editing Users                                                        | 12-58 |
| Deleting Users                                                       | 12-58 |
| Disabling Access to Sensitive Information in Message Tracking        | 12-59 |
| Additional Commands to Support Multiple Users: who, whoami, and last | 12-59 |
| Configuring Restrictive User Account and Password Settings           | 12-61 |
| Changing Passwords                                                   | 12-66 |
| External Authentication                                              | 12-66 |
| Enabling LDAP Authentication                                         | 12-67 |
| Enabling RADIUS Authentication                                       | 12-68 |
| Configuring Access to the Security Management Appliance              | 12-70 |
| Configuring IP-Based Network Access                                  | 12-71 |
| Direct Connections                                                   | 12-71 |
| Connecting Through a Proxy                                           | 12-71 |
| Creating the Access List                                             | 12-72 |
| Configuring the Web UI Session Timeout                               | 12-74 |
| Viewing Active Sessions                                              | 12-75 |
| Configuring the Return Address for Generated Messages                | 12-76 |
| Managing Alerts                                                      | 12-76 |
| Overview of Alerts                                                   | 12-77 |
| Alerts: Alert Recipients, Alert Classifications, and Severities      | 12-77 |
| Alert Settings                                                       | 12-78 |
| Alert Delivery                                                       | 12-78 |
| SMTP Routes and Alerts                                               | 12-79 |



|                                                           |       |
|-----------------------------------------------------------|-------|
| Cisco IronPort AutoSupport                                | 12-79 |
| Alert Messages                                            | 12-79 |
| Alert From Address                                        | 12-80 |
| Alert Subject                                             | 12-80 |
| Example Alert Message                                     | 12-80 |
| Managing Alert Recipients                                 | 12-81 |
| Adding New Alert Recipients                               | 12-82 |
| Configuring Existing Alert Recipients                     | 12-82 |
| Deleting Alert Recipients                                 | 12-83 |
| Configuring Alert Settings                                | 12-83 |
| Editing Alert Settings                                    | 12-83 |
| Alert Listing                                             | 12-84 |
| Hardware Alerts                                           | 12-85 |
| System Alerts                                             | 12-85 |
| Changing Network Settings                                 | 12-89 |
| Changing the System Hostname                              | 12-89 |
| The sethostname Command                                   | 12-90 |
| Configuring Domain Name System Settings                   | 12-90 |
| Specifying DNS Servers                                    | 12-91 |
| Multiple Entries and Priority                             | 12-91 |
| Using the Internet Root Servers                           | 12-92 |
| Reverse DNS Lookup Timeout                                | 12-92 |
| DNS Alert                                                 | 12-93 |
| Clearing the DNS Cache                                    | 12-93 |
| Configuring DNS Settings via the Graphical User Interface | 12-93 |
| Configuring TCP/IP Traffic Routes                         | 12-95 |
| Managing Static Routes in the GUI                         | 12-95 |
| Modifying the Default Gateway (GUI)                       | 12-97 |
| Configuring the Default Gateway                           | 12-97 |
| Changing the Admin User's Password                        | 12-97 |

|                                                                             |        |
|-----------------------------------------------------------------------------|--------|
| Configuring the System Time                                                 | 12-98  |
| Time Zone Page                                                              | 12-98  |
| Selecting a Time Zone                                                       | 12-98  |
| Selecting a GMT Offset                                                      | 12-99  |
| Editing Time Settings (GUI)                                                 | 12-100 |
| Editing the Network Time Protocol (NTP) Configuration (Time Keeping Method) | 12-100 |
| Setting System Time Without Using an NTP Server                             | 12-101 |
| Updating Time Zone Files                                                    | 12-101 |
| Defining Time Ranges for Time-Based Policies                                | 12-102 |
| Managing the Configuration File                                             | 12-103 |
| Managing Multiple Appliances with XML Configuration Files                   | 12-103 |
| Managing Configuration Files in the GUI                                     | 12-104 |
| Saving and Exporting the Current Configuration File                         | 12-105 |
| Loading a Configuration File                                                | 12-105 |
| Resetting the Current Configuration                                         | 12-109 |
| CLI Commands for Configuration Files                                        | 12-110 |
| The showconfig, mailconfig, and saveconfig Commands                         | 12-110 |
| The loadconfig Command                                                      | 12-112 |
| The publishconfig Command                                                   | 12-112 |
| The backupconfig Command                                                    | 12-113 |
| Uploading Configuration Changes Using the CLI                               | 12-113 |
| Managing Disk Usage                                                         | 12-115 |
| Maximum Disk Space Available                                                | 12-116 |
| Editing Disk Quotas                                                         | 12-117 |
| Reallocating Monitoring Service Disk Quotas                                 | 12-117 |

## CHAPTER 13

### Logging 13-1

#### Overview 13-1

#### Logging Versus Reporting 13-2

|                                                         |       |
|---------------------------------------------------------|-------|
| Log Types                                               | 13-2  |
| Log Type Comparison                                     | 13-4  |
| Log Retrieval                                           | 13-6  |
| Filename and Directory Structure                        | 13-6  |
| Log Rollover and Transfer Schedule                      | 13-7  |
| Logs Enabled by Default                                 | 13-7  |
| Log Characteristics                                     | 13-8  |
| Timestamps in Log Files                                 | 13-8  |
| Using Configuration History Logs                        | 13-9  |
| Using CLI Audit Logs                                    | 13-10 |
| Using FTP Server Logs                                   | 13-11 |
| Using HTTP Logs                                         | 13-12 |
| Using Cisco IronPort Spam Quarantine Logs               | 13-14 |
| Using Cisco IronPort Spam Quarantine GUI Logs           | 13-15 |
| Using Cisco IronPort Text Mail Logs                     | 13-15 |
| Examples of Text Mail Log Entries                       | 13-17 |
| Generated or Rewritten Messages                         | 13-23 |
| Sending a Message to the Cisco IronPort Spam Quarantine | 13-24 |
| Using NTP Logs                                          | 13-25 |
| Using Reporting Logs                                    | 13-26 |
| Using Reporting Query Logs                              | 13-27 |
| Using Safelist/Blocklist Logs                           | 13-29 |
| Using SMA Logs                                          | 13-30 |
| Using Status Logs                                       | 13-31 |
| Reading Status Logs                                     | 13-32 |
| Using System Logs                                       | 13-35 |
| Understanding Tracking Logs                             | 13-36 |
| Log Subscriptions                                       | 13-36 |
| Configuring Log Subscriptions                           | 13-37 |
| Setting the Log Level                                   | 13-38 |

|                                                          |       |
|----------------------------------------------------------|-------|
| Creating a Log Subscription in the GUI                   | 13-39 |
| Editing Log Subscriptions                                | 13-41 |
| Configuring Global Settings for Logging                  | 13-41 |
| Logging Message Headers                                  | 13-43 |
| Configuring Global Settings for Logging by Using the GUI | 13-44 |
| Rolling Over Log Subscriptions                           | 13-45 |
| Rolling Over Log Subscriptions Using the GUI             | 13-45 |
| Rolling Over Log Subscriptions via the CLI               | 13-45 |
| Viewing the Most Recent Log Entries in the GUI           | 13-46 |
| Viewing the Most Recent Entries in Logs (tail Command)   | 13-46 |
| Example                                                  | 13-47 |
| Configuring Host Keys                                    | 13-48 |

## APPENDIX A

### Accessing the Appliance A-1

|                                      |     |
|--------------------------------------|-----|
| IP Interfaces                        | A-1 |
| Configuring IP Interfaces            | A-2 |
| Creating IP Interfaces Using the GUI | A-3 |
| FTP Access                           | A-5 |
| Secure Copy (scp) Access             | A-8 |
| Accessing via a Serial Connection    | A-9 |

## APPENDIX B

### Assigning Network and IP Addresses B-1

|                                                         |     |
|---------------------------------------------------------|-----|
| Ethernet Interfaces                                     | B-1 |
| Selecting IP Addresses and Netmasks                     | B-2 |
| Sample Interface Configurations                         | B-2 |
| IP Addresses, Interfaces, and Routing                   | B-3 |
| Summary                                                 | B-4 |
| Strategies for Connecting Your Cisco IronPort Appliance | B-4 |

---

**APPENDIX C****Firewall Information C-1**

---

**APPENDIX D****Examples D-1****Web Security Appliance Examples D-1****Example 1: Investigating a User D-2****Related Topics D-6****Example 2: Tracking a URL D-7****Related Topics D-8****Example 3: Investigating Top URL Categories Visited D-8****Related Topics D-12****Example 4: Privacy and Hiding User Names D-12****Related Topics D-15****Example 5: Upgrading to a New Configuration Master on an Existing Security Management Appliance D-15****Related Topics D-17****Example 6: Importing a Configuration File from an Existing Web Security Appliance D-17****Further Considerations D-19****Related Topics D-20****Example 7: Customizing Access Policies on Remote Web Security Appliances and Managing Them on a Central Security Management Appliance D-20****Set Up the Access Rules D-23****Decide Where the Access Rules Apply D-27****Create the Identities D-28****Create A Custom URL Category for Configuration Master 5.7 D-30****Create the Access Policies and Add Identities D-32****Create the Delegated Administrators D-35****Related Topics D-39**

---

**APPENDIX E**

**Interactive Columns E-1**

[Interactive Columns for the Centralized Web Reporting Pages E-1](#)

[Interactive Columns for the Centralized Email Reporting Pages E-5](#)

---

**APPENDIX F**

**Cisco IronPort End User License Agreement F-1**

[Cisco IronPort Systems, LLC Software License Agreement F-1](#)

---

**INDEX**



# CHAPTER 1

## Getting Started with the Security Management Appliance

---

The *IronPort AsyncOS for Security Management User Guide* provides instructions for setting up, administering, and monitoring the Cisco IronPort Security Management appliance. These instructions are designed for an experienced system administrator with knowledge of networking and email and web administration.

This preface discusses the following topics:

- [Security Management Appliance Overview](#)
- [What's New in This Release](#)
- [How to Use This Guide](#)
- [Before You Begin](#)
- [Document Conventions](#)
- [Where to Find More Information](#)
- [Third Party Contributors](#)
- [Cisco IronPort Welcomes Your Comments](#)

## Security Management Appliance Overview

In the ever increasing complexity of security deployments, even small organizations have a complex organizational infrastructure of on premise systems, managed services, remote workers, and outside partners to collaborate with.

Ensuring a cohesive security and corporate compliance posture across a distributed enterprise requires more than just putting the right components in place. You need a management system that takes all of this complexity into account.

You need flexible policy configuration, comprehensive monitoring, insightful reporting and efficient troubleshooting.

The Security Management appliance is a unified management platform that manages email and web security, performs troubleshooting, as well as maintaining space for data storage for months or even years.

Designed to monitor corporate policy settings and audit information, the Cisco IronPort Security Management appliance combines hardware, an operating system (AsyncOS), and supporting services for Cisco IronPort Email Security appliance (ESA) and Web Security appliances (WSA).

The Security Management appliance centralizes and consolidates important policy and runtime data, providing administrators and end users with a single interface for managing reporting and auditing information for Web Security appliances and Email Security appliances. In addition, you can centrally manage policy definition and policy deployment for up to 150 Web Security appliances.

The Security Management appliance ensures top performance from Email Security appliances and Web Security appliances and protects corporate network integrity by increasing deployment flexibility. You can coordinate your security operations from a single Security Management appliance or spread the load across multiple appliances.

The Security Management appliance offers stability, scalability and speed. The Security Management appliance is a single management platform for the Web Security appliance and the Email Security appliance that provides insight, control and flexibility to email and web security administrators for the appliances on their system.

**Note**

While the Security Management appliance is a robust appliance for centralized tracking, reporting and quarantine management, we do not recommend using the Security Management appliance for centralized email management, or ‘clustering’.



# Supported Services on the Security Management Appliance

The Security Management appliance supports the following services:

- [Email Security Management](#)
- [Web Security Management](#)
- [Additional Features](#)

## Email Security Management

For email administrators, insight into the network is crucial for email management and is provided by reporting. Email reports fulfill two important functions for email administrators:

- to show a wholistic view of email tracking across the network
- to quantify intuitive reports that correlates data from multiple security services such as anti-virus, spam, and incoming or outgoing mail usage counters.

Reports also provide statistics on blocked spam, and email borne threats. Other reports help you stay compliant with corporate policies by providing insight into internal user behavior. These reports then can be converted into PDFs at the click of a button, or you can schedule reports for easy email delivery or can be exported to CSV for further email processing.

The Security Management appliance provides comprehensive insight by collecting data from multiple Email Security appliances in near real time. Insight does not stop at reporting. Detailed message tracking helps you with compliance, and answer questions such as: ‘What happened to the email that I sent an hour ago’.

The Security Management appliance provides an intuitive user interface, rapid search results, and an interactive refinement of searches that helps an email administrators spend less time on mundane search task.

Control for Email Security appliances is provided on the Security Management appliance through the Centralized Management feature. This feature, available on the Email Security appliance, allows you to centrally maintain coherent and cohesive policies. Because administrators want to have a unique policy depending

upon the user, LDAP group membership, or even domain membership. Now you can have that level of policy assignment. Role-based access allows you to distribute monitoring tasks.

The Security Management appliance features a centralized spam quarantine, that empowers end users so that they can manage their own quarantines.

## Web Security Management

For Web Security administrators, malware programs and suspicious web sites on their network are of extreme concern. The Web Security appliance is a robust, secure, efficient device that protects corporate networks against web-based malware and spyware programs that can compromise corporate security and expose intellectual property. The Web Security appliance extends Cisco IronPort's SMTP security applications to include protection for standard communication protocols, such as HTTP, HTTPS, and FTP.

To access information about malicious programs or web sites, reporting is available on the Security Management appliance. This provides comprehensive security reports that provides the system administrator insight into malware threats. Additionally, compliance reports allow you to see if any employees have accessed any unacceptable URL Categories. Control of these and other reports on the Web Security appliances is a very important feature of the Security Management appliance.

Web administrators want to apply consistent acceptable use and security policies across an organization. Policies can be pushed from the Security Management appliance to multiple security appliances running multiple AsyncOS versions. This provides consistent policy applications, even during staged network upgrades. Features that distribute responsibility amongst different employees of an organization provide overall policy control with local overrides. Role based access control, and delegated administration provide a Web administrator with flexibility and fine grained protection.

Additionally, a web administrator can audit policy changes and back up historical policies.

## Additional Features

The AsyncOS for Security Management also incorporates the following features:

- **External Cisco IronPort Spam Quarantine:** Hold spam and suspected spam messages for end users, and allow end users and administrators to review messages that are flagged as spam before making a final determination.
- **Centralized reporting:** Run reports on aggregated data from multiple Email and Web Security appliances.
- **Centralized tracking:** Track email and web messages that traverse multiple Email and Web Security appliances.
- **Cisco IronPort Centralized Configuration Manager:** Manage policy definition and policy deployment for multiple Email and Web Security appliances.

## What's New in This Release

This section describes the new features and enhancements in AsyncOS 7.7 for Security Management. For more information about the release, see the product release notes, which are available at the following URL:

[http://www.cisco.com/en/US/products/ps10155/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html)

You might also find it useful to review release notes for earlier releases to see the features and enhancements that were previously added. Release notes for all releases are available at the link above.

**Table 1-1** summarizes the new features and enhancements that are included in this version of AsyncOS for Security Management.

**Table 1-1 New Features for AsyncOS 7.7 for Security Management**

| Feature                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>New Features:</b>                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Custom Email User Roles for Delegated Administration | <p>In AsyncOS 7.7, you can design custom user roles for administrative access to the following email security-related features on the Security Management appliance:</p> <ul style="list-style-type: none"> <li>• All email reports (optionally restricted by Reporting Group)</li> <li>• Mail policy reports (optionally restricted by Reporting Group)</li> <li>• DLP reports (optionally restricted by Reporting Group)</li> <li>• Message tracking</li> <li>• Spam quarantine</li> </ul> <p>For more information, see the <a href="#">`Delegating Administration with Custom User Roles`</a> section in <a href="#">Chapter 12, `Common Administrative Tasks.`</a></p> |
| Technician Role                                      | <p>New in AsyncOS 7.7, the predefined Technician role allows users to perform system upgrades, reboot the appliance, manage feature keys, and perform other tasks required to upgrade the Security Management appliance.</p> <p>For more information, see the <a href="#">`User Roles`</a> section in <a href="#">Chapter 12, `Common Administrative Tasks.`</a></p>                                                                                                                                                                                                                                                                                                       |
| DLP Tracking Privileges                              | <p>AsyncOS 7.7 allows on-Administrator users to view content in Message Tracking that matches a DLP policy violation. You can enable or disable this access to control visibility of sensitive information.</p> <p>For more information, see the <a href="#">`Disabling Access to Sensitive Information in Message Tracking`</a> section in <a href="#">Chapter 12, `Common Administrative Tasks.`</a></p>                                                                                                                                                                                                                                                                 |
| Restrictive User Accounts and Password Settings      | <p>AsyncOS 7.7 allows you to define user account and password restrictions to enforce organizational password policies. The available password restrictions include mandatory characters, password length, and password lifetime. You can also define how many failed login attempts cause the user to be locked out of the account.</p> <p>For more information, see the <a href="#">`Configuring Restrictive User Account and Password Settings`</a> section in <a href="#">Chapter 12, `Common Administrative Tasks.`</a></p>                                                                                                                                           |

**Table 1-1**      ***New Features for AsyncOS 7.7 for Security Management (continued)***

| <b>Feature</b>                | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP-Based Access               | <p>In AsyncOS 7.7, you can control from which IP addresses users access the Security Management appliance. Users can access the appliance from any machine with an IP address from an access list that you define. If your organization's network uses reverse proxy servers between remote users' machines and the Security Management appliance, AsyncOS 7.7 allows you to create an access list with the IP addresses of the proxies that can connect to the appliance.</p> <p>For more information, see the '<a href="#">Configuring IP-Based Network Access</a>' section in <a href="#">Chapter 12, 'Common Administrative Tasks.'</a></p> |
| Web UI Session Timeout        | <p>AsyncOS 7.7 allows you to specify how long a user can be logged into the Security Management appliance's Web UI before AsyncOS logs the user out due to inactivity. This Web UI session timeout applies to all users, including admin, and it is used for both HTTP and HTTPS sessions.</p> <p>For more information, see the '<a href="#">Configuring the Web UI Session Timeout</a>' section in <a href="#">Chapter 12, 'Common Administrative Tasks.'</a></p>                                                                                                                                                                              |
| Packet Capture                | <p>AsyncOS 7.7 provides packet capture controls, letting you intercept and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached. This feature can help you debug the network setup and to discover what network traffic is reaching or leaving the appliance.</p> <p>For more information, see the '<a href="#">Packet Capture</a>' section in <a href="#">Chapter 2, 'Setup and Installation.'</a></p>                                                                                                                                                                           |
| Timezone Updates              | <p>Effective in AsyncOS 7.7, time zone files can be updated independently of AsyncOS upgrades. You can check for time zone file updates and update time zones manually on the Management Appliance &gt; System Administration &gt; Time Settings page.</p> <p>For more information, see the '<a href="#">Updating Time Zone Files</a>' section in <a href="#">Chapter 12, 'Common Administrative Tasks.'</a></p>                                                                                                                                                                                                                                |
| <b>Enhancements:</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Virus Outbreak Filters Report | <p>The Virus Outbreak Filters report has been enhanced and renamed to the Outbreak Filters Report. This report now also includes information on malware distribution, scams, and phishing attempts.</p> <p>For more information, see the '<a href="#">Outbreak Filters Page</a>' section in <a href="#">Chapter 4, 'Using Centralized Email Reporting.'</a></p>                                                                                                                                                                                                                                                                                 |

**Table 1-1**      ***New Features for AsyncOS 7.7 for Security Management (continued)***

| Feature                  | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PDF Reports Enhancements | <p>New in AsyncOS 7.7, you can generate PDF reports in languages other than English and properly render all non-ASCII characters in PDF reports. PDF reports containing multiple reports now include links at the top of the PDF.</p> <p>For more information, see the <a href="#">`Understanding the Email Reporting Pages'</a> section in <a href="#">Chapter 3, `Appliance Configuration.'</a></p> |
| Attachment Search        | <p>AsyncOS 7.7 allows you to search for messages by attachment name in Message Tracking.</p> <p>For more information, see <a href="#">Chapter 6, `Tracking Email Messages.'</a></p>                                                                                                                                                                                                                   |

## How to Use This Guide

Use this guide as a resource to learn about the features of your Cisco IronPort appliance. The topics are organized in a logical order. You might not need to read every chapter in the book. Review the Table of Contents 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 network and firewall configuration settings, 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 **Help** and **Support** in the upper-right corner.

## Before You Begin

Before you read this guide, review the *IronPort Quickstart Guide* and the latest product release notes for your appliance. In this guide, it is assumed that you have unpacked the appliance, physically installed it in a rack, and turned it on.

If you have already cabled your appliance to your network, ensure that the default IP address for the IronPort appliance does not conflict with other IP addresses on your network.

## Email Security Appliances

For the following Email Security appliances, the preconfigured IP address on Data 1 port is 192.168.42.42.

- X1000T
- C650
- C350

The Cisco IronPort X1050, C650, and C350 appliances are equipped with as many as four Ethernet interfaces located on the rear panel of the system, depending on the configuration (whether or not you have the optional optical network interface). They are labeled:

- Management
- Data1
- Data2
- Data3
- Data4

## Web Security Appliances

For the following Web Security appliances, the preconfigured IP address is 192.168.42.42.

- S1050
- S650
- S350

The Cisco IronPort S1050, S650, and S350 appliances are equipped with as the following Ethernet interfaces located on the rear panel of the system:

- M1

- P1
- P2
- T1
- T2

## Security Management Appliances

For the following Security Management appliances, the preconfigured IP address on Data port 1 is 192.168.42.42

- M160
- M600
- M650
- M660
- M670
- M1000
- M1050
- M1060

## Document Conventions

Command descriptions use these conventions:

- Braces ( { } ) indicate a required choice.
- Square brackets ( [ ] ) indicate optional elements.
- Vertical bars ( | ) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen font`.



- Information you need to enter in examples is shown in **boldface screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

## Where to Find More Information

Cisco IronPort offers the following resources to learn more about the Security Management appliance and related products:

- [Documentation Set, page 1-11](#)
- [Cisco IronPort Technical Training, page 1-12](#)
- [Knowledge Base, page 1-13](#)
- [Cisco Support Community, page 1-14](#)
- [Cisco IronPort Customer Support, page 1-14](#)

## Documentation Set

The documentation set for Cisco IronPort appliances includes the following documents and books (not all types are available for all appliances and releases):

- Release Notes for all products
- Quickstart and Getting Started guides
- *Cisco IronPort AsyncOS for Security Management User Guide* (this book)
- *Cisco IronPort AsyncOS for Web Security User Guide*
- Cisco IronPort AsyncOS for Email Security user guides:
  - *Cisco IronPort AsyncOS for Email Security Configuration Guide*
  - *Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*
  - *Cisco IronPort AsyncOS for Email Security Daily Management Guide*

- *Cisco IronPort AsyncOS CLI Reference Guide*
- Safety and compliance information
- Plug-in and API documentation
- Information about hardware and firmware
- White papers
- Solution guides

Occasionally, this book refers to the other guides for additional information about topics.

Find documentation for Cisco IronPort appliances at the following locations:

| Documentation For:                                    | Is Located At:                                                                                                                                                                    |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Management appliances                        | <a href="http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html</a> |
| Email Security appliances and the CLI reference guide | <a href="http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html</a> |
| Web Security appliances                               | <a href="http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html</a> |

## Cisco IronPort Technical Training

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

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

**Training.** For question relating to registration and general training:

- <http://training.ironport.com>
- [training@ironport.com](mailto:training@ironport.com)

**Certifications.** For questions relating to certificates and certification exams:

- <http://training.ironport.com/certification.html>
- [certification@ironport.com](mailto:certification@ironport.com)

## Knowledge Base

Access the Customer Support Portal, which offers resources including the Cisco IronPort Knowledge Base, at the following URL:

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



### Note

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

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.

## Cisco Support Community

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

Access the Cisco Support Community at the following URL:

<https://supportforums.cisco.com>

## Cisco IronPort Customer Support

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

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

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

U.S. Toll-free: 1 (877) 646-4766

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

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

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

## Third Party Contributors

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

The full text of these agreements can be found here (after logging into the Cisco IronPort Support Portal):

[https://support.ironport.com/3rdparty/AsyncOS\\_User\\_Guide-1-1.html](https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html).

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

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

## 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:

[contentsecuritydocs@cisco.com](mailto:contentsecuritydocs@cisco.com)

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





## CHAPTER 2

# Setup and Installation

---

This chapter guides you through the process of setting up your Security Management appliance by using the System Setup Wizard. Before you follow the procedures in this chapter, complete the steps described in the *Cisco IronPort M-Series Quickstart Guide* that came with your appliance.



### Note

---

After you run the System Setup Wizard, you need to configure the Security Management appliance, the Email Security appliances, and the Web Security appliances before you can use the management features, such as centralized tracking or the Cisco IronPort Centralized Configuration Manager. For information about configuring Cisco IronPort appliances, see [Chapter 3, “Appliance Configuration.”](#)

---

This chapter contains the following sections:

- [Installation Planning, page 2-2](#)
- [Preparing for Setup, page 2-5](#)
- [Accessing the Graphical User Interface, page 2-8](#)
- [Understanding the System Setup Wizard, page 2-9](#)
- [Running the System Setup Wizard, page 2-11](#)
- [Security Management Appliance User Interface, page 2-17](#)
- [Accessing Customer Support from the Security Management Appliance, page 2-20](#)
- [SMA Compatibility Matrix, page 2-32](#)

# Installation Planning

The Security Management appliance lets you separate end user applications from the more secure gateway systems residing in your demilitarized zones (DMZs). Using a two-layer firewall can provide flexibility in network planning so that end users do not connect directly to the outer DMZ (see [Figure 2-1](#)).

**Figure 2-1** *Typical Network Configuration Incorporating the Security Management appliance*

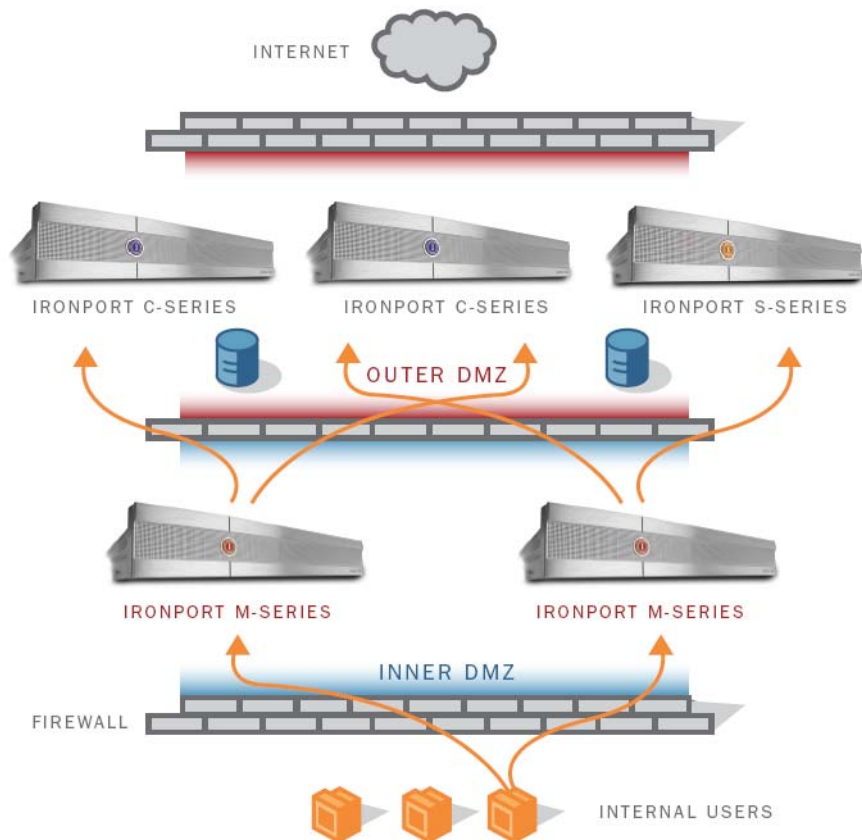




Figure 2-1 shows a typical network configuration incorporating the Security Management appliance and multiple DMZs. You deploy the Security Management appliance outside your DMZ, in your internal networks. All connections are initiated by the Security Management appliances (Cisco IronPort M-Series) to the managed Email Security appliances (Cisco IronPort C-Series) and managed Web Security appliances (Cisco IronPort S-Series).

Corporate data centers can share a Security Management appliance to perform centralized reporting and message tracking for multiple Web and Email Security appliances, and centralized policy configuration for multiple Web Security appliances. The Security Management appliance can also be used as an external Cisco IronPort Spam Quarantine.

After you connect the Email Security appliance and the Web Security appliances to a Security Management appliance and properly configure all appliances, AsyncOS gathers and aggregates data from the managed appliances. From the aggregated data, reports can be generated and an overall view of email and web usage can be determined.

## Mail Flow When Using the Security Management Appliance as an External Spam Quarantine

Mail is sent to the Security Management appliance from the Email Security appliances. An Email Security appliance that sends mail to a Security Management appliance does not reprocess the messages when it receives them back from the Security Management appliance; the messages bypass the HAT and other policy or scanning settings. For this to work, the IP address of the Security Management appliance must be the same for both receiving and sending messages. Otherwise, when an Email Security appliance receives messages from the Security Management appliance, it would process the message again as if it were another incoming message.



---

**Note**

Always use the same IP address for receiving and sending on the Security Management appliance.

---

The Security Management appliance accepts mail for quarantining from the IP addresses specified in the Cisco IronPort Spam Quarantine settings. To configure the local quarantine on the Security Management appliance, see the [“Configuring Cisco IronPort Spam Quarantine Settings” section on page 7-3](#).

**Note**

The local quarantine on the Security Management appliance is referred to as an *external* quarantine by the other Cisco IronPort appliances sending mail to it.

Mail released by the Security Management appliance is delivered to the primary and secondary hosts (Cisco IronPort appliance or other groupware host) as defined in the spam quarantine settings (see the [“Configuring Cisco IronPort Spam Quarantine Settings” section on page 7-3](#)). Regardless of the number of Cisco IronPort appliances delivering mail to the Security Management appliance, all released mail, notifications, and alerts are sent to a single host (groupware or Cisco IronPort appliance). Take care not to overburden the primary host for delivery from the Security Management appliance.

## Centralized Management and the Security Management Appliance

The Security Management appliance cannot be placed in a cluster. However, clustered Cisco IronPort appliances can deliver messages to the Security Management appliance for centralized reporting and tracking and to store the messages in an external spam quarantine.

## Physical Dimensions

The following physical dimensions apply to the **Cisco IronPort M1000/1050 and M600/650** Security Management appliances:

- Height: 8.656 cm (3.40 inches)
- Width: 48.26 cm (19.0 inches) with rails installed (without rails, 17.5 inches)
- Depth: 75.68 cm (29.79 inches)
- Weight: maximum 26.76 kg (59 pounds)

The following physical dimensions apply to the **Cisco IronPort M1070 and 670** Security Management appliances:

- Height: 8.64 cm (3.40 inches)
- Width: 48.24 cm (18.99 inches) with rails installed (with or without rails)
- Depth: 72.06 cm (28.40 inches)
- Weight: maximum 26.76 kg (59 pounds)

The following physical dimensions apply to the **Cisco IronPort M160** Security Management appliance:

- Height: 4.20 cm (1.68 inches)
- Width: 48.26 cm (19.00 inches) with rails installed (without rails 17.5 inches)
- Depth: 57.60 cm (22.70 inches)
- Weight: maximum 7.80 kg (21.6 pounds)

## Preparing for Setup

To set up the Security Management appliance, you need to use the System Setup Wizard in the graphical user interface (GUI). The Security Management appliance does not support system setup through the command line interface (CLI). For more information about running the wizard, see the [“Understanding the System Setup Wizard” section on page 2-9](#).

Before you can log in to the GUI, you need to set up a private connection between a PC and the Security Management appliance. For example, you can use the included crossover cable to connect directly from the Management port on the appliance to a laptop. Optionally, you can connect through an Ethernet connection between a PC and the network (for example, an Ethernet hub) and between the network and the Management port on the Security Management appliance. The factory assigned IP address of the Management port is 192.168.42.42. After setup, go to the **Management Appliance > Network > IP Interfaces** page on the main Security Management appliance to change the interface that the Security Management appliance uses.

## Understanding the System Setup Steps

To set up the Security Management appliance:

- 
- |               |                                                                 |
|---------------|-----------------------------------------------------------------|
| <b>Step 1</b> | Determine network and IP address assignments.                   |
| <b>Step 2</b> | Gather information about your system setup.                     |
| <b>Step 3</b> | Launch a web browser and enter the IP address of the appliance. |
| <b>Step 4</b> | Run the System Setup Wizard to configure the system.            |
- 

## Determining Network and IP Address Assignments

You need the following network information about each Ethernet port that you choose to use:

- IP address
- Netmask

In addition, you need the following information about your overall network:

- IP address of the default router (gateway) on your network
- IP address and hostname of your DNS servers (not required if you want to use Internet root servers)
- Hostname or IP address of your NTP servers (not required if you want to manually set system time)

For more information, see [Appendix B, “Assigning Network and IP Addresses.”](#)

**Note**

---

If you are running a firewall on your network between the Internet and the Cisco IronPort appliance, it may be necessary to open specific ports for the Cisco IronPort appliance to work properly. For more information on firewalls, see [Appendix C, “Firewall Information.”](#)

---

## Gathering the Setup Information

Use the following table to gather information about system setup. You will need this information at hand while running the System Setup Wizard.


**Note**

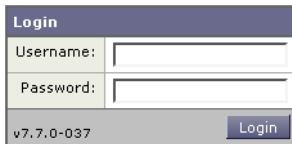
See the [Appendix B, “Assigning Network and IP Addresses,”](#) for detailed information about network and IP addresses.

**Table 2-1**      **System Setup Worksheet**

|   |                        |                                                                |
|---|------------------------|----------------------------------------------------------------|
| 1 | Notifications          | Email address where system alerts are sent:                    |
| 2 | System Time            | NTP Server (IP address or hostname):                           |
| 3 | Admin Password         | Choose a new password for the “admin” account:                 |
| 4 | AutoSupport            | Enable Cisco IronPort AutoSupport? ___ Yes ___ No              |
| 5 | Hostname               | Fully qualified hostname of the Security Management appliance: |
| 6 | Interface / IP Address | IP address:                                                    |
|   |                        | Netmask:                                                       |
| 7 | Network                | Gateway                                                        |
|   |                        | DNS                                                            |
|   |                        | Default Gateway (router) IP address:                           |
|   |                        | ___ Use the Internet’s root DNS servers                        |
|   |                        | ___ Use these DNS servers:                                     |

# Accessing the Graphical User Interface

- Step 1** To access the graphical user interface on the Security Management appliance, open your web browser and type **192.168.42.42** in the IP address text field. The login screen is displayed.



- Step 2** Log in to the Security Management appliance by entering the following factory-assigned user name and password in the corresponding text fields.
- User name: **admin**
  - Password: **ironport**



## Note

Your session times out if you are idle for more than 30 minutes or if you close the browser without logging out. If this happens, you must reenter your user name and password. If the session times out while you are running the System Setup Wizard, you need to start over from the beginning.

## Accessing the Web Interfaces of the Security Management Appliance

The Security Management appliance has two web interfaces: the standard administrator interface, available by default on port 80, and the Cisco IronPort Spam Quarantine end user interface, available by default on port 82. The Cisco IronPort Spam Quarantine HTTPS interface defaults to port 83 once enabled.

Because you can specify HTTP or HTTPS when configuring each of the web interfaces (go to **Management Appliance > Network > IP Interfaces** on the Security Management appliance), you may be asked to reauthenticate if you switch between the two during your session. For example, if you access the admin

web interface through HTTP on port 80 and then, in the same browser, access the Cisco IronPort Spam Quarantine end user web interface through HTTPS on port 83, you are asked to reauthenticate if you return to the admin web interface.

## Accessing the Security Management Appliance Command Line Interface

The command line interface, or CLI, is accessed on the Security Management appliance in the same way that the CLI is accessed on all Cisco IronPort appliances. There are, however, some differences:

- System setup *must* be performed through the GUI.
- Some CLI commands are not available on the Security Management appliance. For a list of which commands are not supported, see the *Cisco IronPort AsyncOS CLI Reference Guide*.

## Understanding the System Setup Wizard



### Warning

**The System Setup Wizard completely reconfigures the appliance. Only use the wizard when you initially install the appliance, or if you want to completely overwrite the existing configuration.**

AsyncOS provides a browser-based System Setup Wizard to guide you through the process of system configuration. Later, you may want to take advantage of custom configuration options not available in the wizard. However, you *must* use the wizard for the initial setup to ensure a complete configuration. If you gather the required information in [Table 2-1](#) before you run the System Setup Wizard, you can complete the setup quickly and easily.

Be sure to connect the Security Management appliance to your network through the Management port.

**Warning**

---

**The Security Management appliance ships with a default IP address of 192.168.42.42 on the Management port. Before connecting the Security Management appliance to your network, ensure that no other device's IP address conflicts with the factory default setting.**

---

## Browser Requirements

To access the GUI, your browser must support and be enabled to accept JavaScript and cookies, and it must be able to render HTML pages containing Cascading Style Sheets (CSS). Specifically:

- Firefox 1.0 and higher
- Windows XP: IE 6.02 and higher
- Windows Vista: Internet Explorer 7.0 and higher
- Mozilla 1.76 and higher
- Netscape 7.1 and later
- Mac OS X: Safari 2.0.4 and later
- Opera 10.0.x

The GUI requires a minimum browser size of 1024x768 pixels.

**Note**

---

Conditional support is offered for Internet Explorer 6.0 and Opera 10.0.x on the Windows XP operating system and for Safari 3.1 on Mac OS X. Conditional support means that important functional bugs will be addressed, but minor or visual issues may not be corrected.

---

Your session will automatically time out after 30 minutes of inactivity.

**Note**

---

When accessing the GUI, do not use multiple browser windows or tabs simultaneously to make changes to the Security Management appliance. Do not use concurrent GUI and CLI sessions either. Doing so will cause unexpected behavior and is not supported.

---



You may need to configure your browser's pop-up blocking settings in order to use the GUI, because some buttons or links in the interface will cause additional windows to open.

## Support Languages

With the appropriate license key, AsyncOS can display the GUI and CLI in any of the following languages:

- English
- French
- Spanish
- German
- Italian
- Korean
- Japanese
- Portuguese (Brazil)
- Chinese (zh-cn and zh-tw)
- Russian

## Running the System Setup Wizard

To launch the wizard, log in to the GUI as described in the [“Browser Requirements” section on page 2-10](#). The first time you log in to the GUI, the initial page of the System Setup Wizard appears by default. You can also access the System Setup Wizard from the System Administration menu.

The System Setup Wizard leads you through the following configuration tasks:

- 
- |               |                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Reviewing the end user license agreement                                                                                                                          |
| <b>Step 2</b> | Configuring the following system settings: <ul style="list-style-type: none"><li>– Notification settings and AutoSupport</li><li>– System time settings</li></ul> |

- Admin password
- Step 3** Configuring the following network settings:
- Hostname of the appliance
  - IP address, network mask, and gateway of the appliance
  - Default router and DNS settings

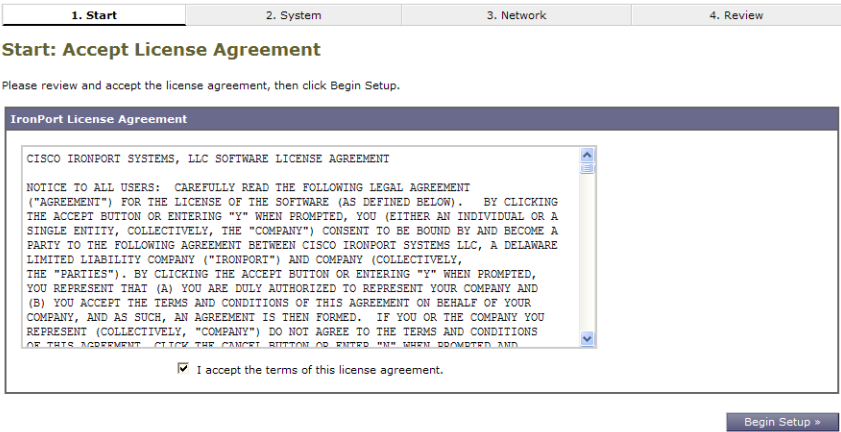
**Step 4** Reviewing your configuration

Proceed through the wizard pages, and carefully review your configuration at step 4. You can return to a step by clicking **Previous**. At the end of the process, the wizard prompts you to commit the changes that you have made. Most changes do not take effect until you commit them.

## Step 1: Review the End User License Agreement

Begin by reading the license agreement. After you have read and agreed to the license agreement, select the check box indicating that you agree, and then click **Begin Setup** to proceed.

**Figure 2-2** *Reviewing the License Agreement*



## Step 2: Configure the System Settings

When you begin setup in the System Setup Wizard, the System Configuration page appears. This page allows you to configure the system settings.

**Figure 2-3** *Configuring System Settings with the System Configuration Page*

|          |                  |            |           |
|----------|------------------|------------|-----------|
| 1. Start | <b>2. System</b> | 3. Network | 4. Review |
|----------|------------------|------------|-----------|

### System Configuration

Before you begin, you should consult the "Enabling Your IronPort M-Series Security Management Appliance" chapter in the AsyncOS User Guide.

| System Settings         |                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Email system alerts to: | <input type="text" value="e.g. admin@company.com"/>                                                                                                      |
| Time Zone:              | Region: <input type="text" value="GMT Offset"/><br>Country: <input type="text" value="GMT"/><br>Time Zone / GMT Offset: <input type="text" value="GMT"/> |
| NTP Server:             | <input type="text" value="time.ironport.com"/>                                                                                                           |
| Administrator Password: | Password: <input type="password"/><br><small>Must be 6 or more characters.</small><br>Confirm Password: <input type="password"/>                         |
| AutoSupport: (?)        | <input checked="" type="checkbox"/> Send system alerts and weekly status reports to IronPort Customer Support (recommended)                              |

Cancel Next »

### Configuring Email System Alerts

AsyncOS sends alert messages through email if there is a system error that requires the user's intervention. Enter the email address (or addresses) where the alerts are sent.

You need to add at least one email address for the system alerts. Separate multiple addresses with commas. The email addresses that you enter initially receive all types of alerts at all levels. You can customize the alert configuration later. For more information, see the [“Managing Alerts” section on page 12-76](#).

### Setting the Time

Set the time zone on the Security Management appliance so that timestamps in message headers and log files are correct. Use the drop-down menus to locate your time zone or to define the time zone by GMT offset.

You can set the system clock time manually, or you can use Network Time Protocol (NTP) to synchronize time with other servers on your network or the Internet. By default, the Cisco IronPort Systems time servers (time.ironport.com) are added as an entry to synchronize the time on your Security Management appliance. Enter the hostname of the NTP server, and click **Add Entry** to configure an additional NTP server. For more information, see the [“Configuring the System Time” section on page 12-98](#).

**Note**

When gathering data for reports, the Security Management appliance applies a time stamp on the data. The time stamp is applied using the configuration settings that you implemented from the steps in the [“Configuring the System Time” section on page 12-98](#).

For more information on how the Security Management appliance gathers data, see the [“How the Security Appliance Gathers Data for Reports” section on page 3-16](#).

## Setting the Password

You must change the password for the AsyncOS admin account. The new password must be six characters or longer. Keep the password in a secure location. Changes to the password take effect immediately.

**Note**

If you cancel the system setup after resetting the password, your password changes are not undone.

## Enabling AutoSupport

The Cisco IronPort AutoSupport feature (enabled by default) notifies Cisco IronPort Customer Support about issues with the Security Management appliance so that they can provide optimal support. For more information, see the [“Cisco IronPort AutoSupport” section on page 12-79](#).

## Step 3: Configure the Network Settings

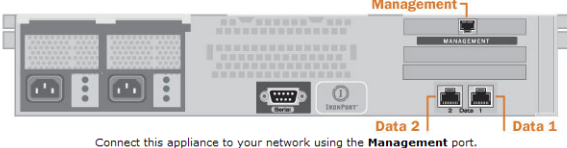
Define the hostname of the machine and then configure the gateway and DNS settings.

**Figure 2-4** Configuring Network Settings

|          |           |            |           |
|----------|-----------|------------|-----------|
| 1. Start | 2. System | 3. Network | 4. Review |
|----------|-----------|------------|-----------|

**System and Network Configuration**

**Network Settings**



Connect this appliance to your network using the **Management** port.

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                             |            |         |  |                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|------------|---------|--|------------------------------------------------------------------------------|
| Hostname:      | sma01-vmw1-tpub.qa                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Fully qualified hostname for this appliance |            |         |  |                                                                              |
| IP Address:    | 172.17.0.212                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                             |            |         |  |                                                                              |
| Network Mask:  | 255.255.255.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                             |            |         |  |                                                                              |
| Gateway:       | 172.17.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                             |            |         |  |                                                                              |
| DNS Server(s): | <input checked="" type="radio"/> Use the Internet's Root DNS Servers (recommended)<br><input type="radio"/> Use the specified DNS Servers: <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="border: 1px solid #ccc; width: 80%;">IP Address</td> <td style="border: 1px solid #ccc; width: 20%; text-align: center;">Add Row</td> </tr> <tr> <td style="border: 1px solid #ccc; height: 20px;"></td> <td style="border: 1px solid #ccc; text-align: center;"> <input type="button" value="Add Row"/> <input type="button" value="Delete"/> </td> </tr> </table> |                                             | IP Address | Add Row |  | <input type="button" value="Add Row"/> <input type="button" value="Delete"/> |
| IP Address     | Add Row                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                             |            |         |  |                                                                              |
|                | <input type="button" value="Add Row"/> <input type="button" value="Delete"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                             |            |         |  |                                                                              |

◀ Previous
Cancel
Next ▶

**Note**

Verify that you have connected the Security Management appliance to your network through the Management port.

## Network Settings

Enter the fully qualified hostname for the Security Management appliance. This name should be assigned by the network administrator.

Enter the IP address of the Security Management appliance.

Enter the network mask and IP address of the default router (gateway) on your network.

Next, configure the Domain Name Service (DNS) settings. AsyncOS contains a high-performance internal DNS resolver/cache that can query the Internet's root servers directly, or the system can use DNS servers that you specify. If you use your own servers, you need to supply the IP address of each DNS server. You can enter up to four DNS servers when you are using the System Setup Wizard.



**Note**

The DNS servers you specify have an initial priority of 0. For more information, see the [“Configuring Domain Name System Settings” section on page 12-90](#).



**Note**

The appliance requires access to a working DNS server to perform DNS lookups for incoming connections. If you cannot specify a working DNS server that is reachable by the appliance while you are setting up the appliance, you can select Use Internet Root DNS Servers, or else temporarily specify the IP address of the Management interface so that you can complete the System Setup Wizard.

**Step 4: Review Your Configuration**

Now, the System Setup Wizard displays a summary of the setup information that you have entered. If you need to make any changes, click **Previous** at the bottom of the page and edit the information.

**Figure 2-5      Reviewing Your Configuration**

1. Start

2. System

3. Network

4. Review

### Review Your Configuration

Please review your configuration. If you need to make changes, click the Previous button to return to the previous page. [Printable Page](#)

| System Settings         |                                                                 |
|-------------------------|-----------------------------------------------------------------|
| System Time:            | NTP Server: time.ironport.com<br>Time Zone: America/Los_Angeles |
| Email system alerts to: |                                                                 |
| AutoSupport:            | Enabled                                                         |

| Network Settings |                    |
|------------------|--------------------|
| Gateway:         | 172.17.0.1         |
| DNS:             | 172.17.0.3         |
| Hostname:        | sma01-vmw1-tpub.qa |
| IP Address:      | 172.17.0.212:6025  |
| Network Mask:    | 255.255.255.0      |

« Previous

Cancel

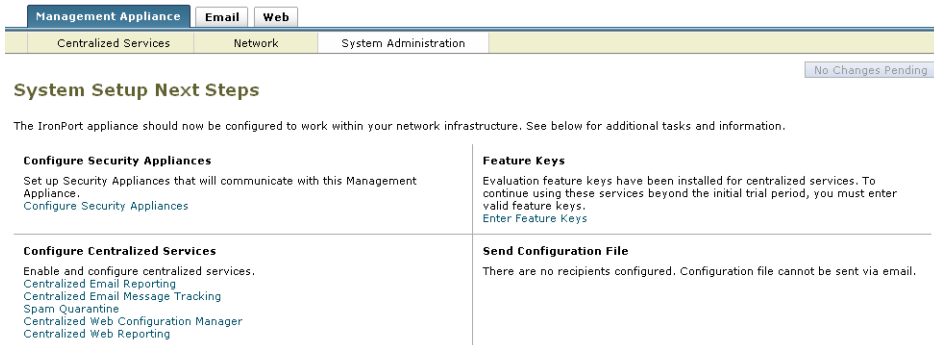
Install This Configuration

After you have reviewed the information, click **Install This Configuration**. Then click **Install** in the confirmation dialog box that appears.

## Proceeding to the Next Steps

If the System Setup Wizard properly installs the configuration on the Security Management appliance, the **System Setup Next Steps** page appears.

**Figure 2-6 System Setup —Next Steps**



Click on any of the links on the System Setup Next Steps page to proceed with the configuration of your Cisco IronPort appliances. For more information about appliance configuration, see [Chapter 3, “Appliance Configuration.”](#)

After you install the Security Management appliance and run the System Setup Wizard, you can modify other settings on the appliance and configure the monitoring services.

For information about configuring the monitoring services, see [Chapter 9, “Monitoring System Status.”](#)

## Security Management Appliance User Interface

The System Status page is the initial page that you view when first logging into the Security Management appliance.

**Figure 2-7 Security Management Appliance Graphical User Interface**

 **IRONPORT M600**

Logged in as: **admin** on **vmw002-esa03.run**  
Options ▾ Help and Support ▾

**Management Appliance** | Email | Web

Centralized Services | Network | System Administration

No Changes Pending

### System Status Printable (PDF)

| Centralized Services                        |                                        |                            |
|---------------------------------------------|----------------------------------------|----------------------------|
| Email Security                              |                                        |                            |
| Spam Quarantine                             |                                        |                            |
| Disk Quota Used: 0.0% <input type="text"/>  | Messages: 0                            | Not enabled                |
| Centralized Reporting                       |                                        |                            |
| Processing Queue: 0.0% <input type="text"/> | Status: Not enabled                    | Email Overview Report      |
| Centralized Message Tracking                |                                        |                            |
| Processing Queue: 0.0% <input type="text"/> | Status: Not enabled                    | Track Messages             |
| Web Security                                |                                        |                            |
| Centralized Configuration Manager           |                                        |                            |
| Last Publish: N/A                           | Status: Never connected (2 Appliances) | View Appliance Status List |
| Centralized Reporting                       |                                        |                            |
| Processing Queue: 0.0% <input type="text"/> | Status: Never connected (2 Appliances) | Web Overview Report        |

| Security Appliance Data Transfer Status |              |      |                   |                                   |
|-----------------------------------------|--------------|------|-------------------|-----------------------------------|
| Appliance                               |              |      | Connection Status |                                   |
| Name                                    | IP Address   | Type | Status ▲          | Services                          |
| wsa-04                                  | 10.92.152.90 | Web  | Never connected   | Centralized Configuration Manager |
| vm-03                                   | 10.92.152.89 | Web  | Never connected   | Centralized Configuration Manager |

| System Information             |                                            |
|--------------------------------|--------------------------------------------|
| Uptime                         |                                            |
| Appliance Up Since:            | 22 Jan 2010 21:01 (GMT)<br>(3d 1h 40m 16s) |
| CPU Utilization                |                                            |
| Security Management Appliance: | 0.0%                                       |
| Quarantine Service:            | 0.0%                                       |
| Reporting Service:             | 1.0%                                       |
| Tracking Service:              | 0.0%                                       |
| <b>Total CPU Utilization:</b>  | <b>1.0%</b>                                |
| Version Information            |                                            |
| Model:                         | M600                                       |
| Operating System:              | 6.9.0-081                                  |
| Build Date:                    | 21 Jan 2010 00:00 (GMT)                    |
| Install Date:                  | 22 Jan 2010 20:18 (GMT)                    |
| Serial Number:                 | 000C29016FA8-vmware                        |
| Hardware                       |                                            |
| RAID Status:                   | Unknown                                    |

The System Status page provides detailed status information for the Security Management appliance, including the following:

- **System Status:** overview of the services (Cisco IronPort Spam Quarantine, centralized reporting, centralized tracking, and centralized configuration manager)
- **System Uptime:** how long the appliance has been running



- **CPU Utilization:** percentage of CPU capacity used by each monitoring service
- **System Version Information:** model number, AsyncOS version, build date, installation date, and serial number

For more information about the System Status page, see [Chapter 9, “Monitoring System Status.”](#)

## Tabs on the System Status Page

The following tabs are available to administrator and operator users on the System Status Page:

- **Management Appliance tab:** Centralized Services (System Status; Security Appliances; Email: Spam Quarantine, Centralized Reporting, Centralized Message Tracking; Web: Centralized Web Reporting, Centralized Configuration Manager), Network (IP Interfaces; SMTP Routes; DNS; Routing), System Administration (Users; User Roles; Alerts; Log Subscriptions; Return Addresses; LDAP; Disk Management; Shutdown/Reboot; Configuration File; System Upgrade; System Time: Time Zone, Time Settings; Feature Keys: Feature Key Settings, Feature Keys, Update Settings; System Setup: System Setup Wizard, Next Steps)
- **Email tab:** Reporting (Overview; Incoming Mail; Outgoing Destinations; Outgoing Senders; Internal Users; DLP Incidents; Content Filters; Virus Types; TLS Connections; Virus Outbreaks; System Capacity; Reporting Data Availability; Scheduled Reports; Archived Reports), Message Tracking (Message Tracking; Message Tracking Data Availability), Message Quarantine (Spam Quarantine)
- **Web tab:** Reporting (Overview: Users; Web Sites; URL Categories; Application Visibility; Security: Anti-Malware; Client Malware Risk, Web Reputation Filters; L4 Traffic Monitor; Reporting by User Location; Reporting Services: Web Tracking; System Capacity; Data Availability; Scheduled Reports, Archived Reports), Utilities (Web Appliance Status; Security Services Display; Configuration Masters; Publish: Publish to Web Appliances, Publish History), Configuration Master 5.7 (Web Security Manager: Identities, Decryption Policies, Routing Policies, Access Policies, Proxy Bypass, Custom URL Categories, Time Ranges), Configuration Master 6.3 (Web Security Manager: Identities, Decryption Policies, Routing Policies, Access Policies; Data Loss Prevention: Cisco IronPort Data Security

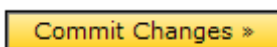
Policies, External DLP Policies; Proxy Bypass; Custom Policy Elements: Custom URL Categories, Time Ranges), Configuration Master 7.1 (Authentication: Identities, SaaS Policy, Web Policies: Decryption Policies, Routing Policies, Access Policies, Overall Bandwidth Limits; Data Loss Prevention: Cisco IronPort Data Security Policies, External DLP Policies, Outbound Malware Scanning; Custom Policy Elements: Custom URL Categories, Time Ranges; Global Settings: Bypass Settings).

When you distribute administration responsibilities to other users, those users can see only the information to which you grant them access. For more information, see [User Roles, page 12-40](#), [Using Custom Email User Roles, page 12-50](#), [About Custom Email User Roles, page 12-45](#), and [About Custom Web User Roles, page 12-51](#).

## Commit Changes Button

As you make configuration changes in the Security Management appliance GUI, you must explicitly commit those changes by clicking **Commit Changes**. If you have not made any changes, then the **No Changes** appears instead of **Commit Changes**.

**Figure 2-8**      *The Commit Changes Button*



Clicking **Commit Changes** displays a page where you can add a comment and commit the changes, abandon all changes made since the most recent commit, or cancel. The color of the **Commit Changes** changes to orange when changes have been submitted.

## Accessing Customer Support from the Security Management Appliance

The following commands and features are useful when you need to contact Customer Support or activate features on the Security Management appliance:

- [Technical Support, page 2-21](#)
- [Working with Feature Keys, page 2-30](#)

## Technical Support

Use the **Help and Support** menu in the upper-right corner of the GUI to access the features related to Cisco IronPort Customer Support.

The technical support features include two pages: the **Open a Support Case** page and the **Remote Access** page.

## Support Request

You can use the Help and **Support > Open a Support Case** page or the **supportrequest** command to email the configuration of your appliance to Customer Support or to other users, and enter comments describing the issue for which you need support. See the *Cisco IronPort AsyncOS CLI Reference Guide* for more information about the **supportrequest** command. This command requires that the appliance is able to send mail to the Internet.

**Figure 2-9 Support Request Page**

**Support Request**

| Request Technical Support                  |                                                                                                                                                                                                                                              |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sent Request to:                           | <input checked="" type="checkbox"/> IronPort Customer Support<br>Other recipients (optional): <input type="text"/><br><i>Separate multiple email addresses with commas.</i>                                                                  |
| Contact Information:                       | Name: <input type="text"/><br>Email: <input type="text"/><br><hr/> Other Contact Information (optional)<br><hr/> Phone1: <input type="text"/><br>Phone2: <input type="text"/><br><i>(Mobile, Pager, etc.)</i><br>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.<br><div style="border: 1px solid #ccc; 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.<br><input type="text"/>                                                                                                                          |

Send

To make a Cisco IronPort Customer Support request:

- Step 1** On the **Help and Support > Open a Support Case** page, enter your contact information (name, email address, and phone numbers).
- Step 2** Enter a description of the issue.
- Step 3** Optionally, enter additional recipients' email addresses in the **Other recipients** field.

By default, the support request (including the configuration file) is sent to Cisco IronPort Customer Support when you select the check box 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 already have a customer support ticket for this issue, enter the ticket number at the bottom of the page.

**Step 5** Click **Send**.

A trouble ticket is automatically created. For additional information, see [Cisco IronPort Customer Support, page 1-14](#).

## Remote Access

Use the Remote Access page to give Cisco IronPort Customer Support remote access to your appliance.

To enable remote access, perform the following steps:

**Step 1** On the right hand side of the Security Management appliance GUI, choose **Help and Support > Remote Access**.

The Customer Support Remote Access window appears.

**Step 2** Select **Edit Remote Access Settings**.

The **Edit Customer Support Remote Access** page appears.

**Figure 2-10** *Edit Customer Support 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"/><br><i>Cannot be the same as your admin password</i>                                       |
| Secure Tunnel (recommended):                                              | <input checked="" type="checkbox"/> Initiate connection via secure tunnel<br>Port: <input type="text" value="25"/> |
| Appliance Serial Number:                                                  | XXXXXXXXXXXX-XXXXXXX                                                                                               |

Cancel
Submit

**Step 3** Check the **Allow remote access to this appliance** check box.**Step 4** Enter your customer support password.**Step 5** Leave the Secure Tunnel check box selected and leave the port number 25, unless a customer support engineer instructs you to change these options.**Step 6** Click **Submit** and then click **Commit** to commit your changes.

By enabling Remote Access you are activating a special account used by 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.cisco.com**. By default this connection is over port 25, which works 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.cisco.com**, Customer Support is able to use the SSH tunnel to obtain access to the appliance. As long as the connection over port 25 is allowed, this bypasses most firewall restrictions. You can also use the **techsupport tunnel** command in the CLI.

In both the Remote Access mode and Tunnel mode, a password is required. It is important to understand that this is *not* the password that will be used to access the system. After that password and the system serial number are provided to your customer support representative, a password used to access the appliance is generated.

After the technical support tunnel is enabled, it remains connected to **upgrades.cisco.com** for seven days. At the end of the seven days, established connections are not disconnected but are unable to reattach to the tunnel once disconnected. The timeout set on the SSH tunnel connection does not apply to the Remote Access account; it remains active until specifically deactivated.

## Packet Capture

Sometimes when you contact Cisco IronPort Customer Support with a Security Management appliance issue, you may be asked to provide insight into the network activity going into and out of the Security Management appliance. The Security Management appliance provides the ability to intercept and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.

You might want to run a packet capture to debug the network setup and to discover what network traffic is reaching the appliance or leaving the appliance.

The appliance saves the captured packet activity to a file and stores the file locally. You can configure the maximum packet capture file size, how long to run the packet capture, and on which network interface to run the capture. You can also use a filter to limit the packet capture to traffic through a specific port or traffic from a specific client or server IP address.

The **Help and Support > Packet Capture** page on the Security Management appliance displays the list of complete packet capture files stored on the hard drive. When the packet capture process 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**.

**Note**

---

In the CLI, use the **packetcapture** command. This command is similar to the **tcpdump** command in UNIX.

---

## Starting a Packet Capture

There are two ways to start a packet capture:

- [Starting a Packet Capture from the Command Line Prompt, page 2-25](#)
- [Starting a Packet Capture from the GUI, page 2-25](#)

### Starting a Packet Capture from the Command Line Prompt

To start a packet capture, type **packetcapture > start** command from the command line prompt. If you need to stop a running packet capture, run the **packetcapture > stop** command. The appliance stops the packet capture when the session ends.

### Starting a Packet Capture from the GUI

To start a packet capture on the Security Management appliance, use the following steps:

**Step 1** On the Security Management appliance, choose **Help and Support > Packet Capture**.

**Step 2** The Packet Capture page is displayed.

| Current Packet Capture        |  |
|-------------------------------|--|
| No packet capture in progress |  |
| Start Capture                 |  |

| Manage Packet Capture Files                          |  |
|------------------------------------------------------|--|
| M650-00188B4B2DAD-861TBC1-20110418-111952.cap (133K) |  |
| Delete Selected Files   Download File                |  |

| Packet Capture Settings  |                          |
|--------------------------|--------------------------|
| Capture File Size Limit: | 200 MB                   |
| Capture Duration:        | Run Capture Indefinitely |
| Interfaces Selected:     | ALL                      |
| Filters Selected:        | No filter                |
| Edit Settings...         |                          |

**Step 3** Select **Start Capture**.

**Step 4** The following figure shows the Packet Capture process running.

#### Packet Capture

Success — Packet capture is started

| Current Packet Capture                                             |  |
|--------------------------------------------------------------------|--|
| Status: Capture in progress (Duration: 3m 8s)                      |  |
| File Name: M650-005056AA1402-vmware-20101208-210129.cap (Size: 0B) |  |
| Current Settings:                                                  |  |
| Max. File Size: 200MB                                              |  |
| Capture Limit: No Limit                                            |  |
| Capture Interfaces: ALL                                            |  |
| Capture Filter: (tcp port 25)                                      |  |
| Stop Capture                                                       |  |

| Manage Packet Capture Files           |  |
|---------------------------------------|--|
|                                       |  |
| 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...         |                          |



To stop a running capture, click **Stop Capture**. A running capture that has previously been started is preserved between sessions.

---

**Note**

The GUI only displays packet captures started in the GUI, not from the command line prompt using the **packetcapture > start** command. Similarly, the command line only displays the status of a current packet capture run started from the command line prompt using the **packetcapture > start** command. Only one capture may be running at a time.

---

## Editing Packet Capture Settings

There are two ways to edit packet capture settings:

- [Editing a Packet Capture Settings from the Command Line Prompt, page 2-27](#)
- [Editing a Packet Capture Settings from the GUI, page 2-27](#)

### Editing a Packet Capture Settings from the Command Line Prompt

To edit the packet capture settings in the CLI, run the **packetcapture > setup** command from the command line prompt.

### Editing a Packet Capture Settings from the GUI

To edit packet capture settings from the GUI, use the following steps:

---

- Step 1** On the Security Management appliance, choose **Help and Support > Packet Capture**.
- The Packet Capture
- Step 2** Select **Edit Settings**..

Step 3 The Edit Packet Capture Settings page appears.

Edit Packet Capture Settings

Packet Capture Settings

Capture File Size Limit: ?

200 MB

Maximum file size is 200MB

Capture Duration:

Run Capture Until File Size Limit Reached

Run Capture Until Time Elapsed Reaches

Run Capture Indefinitely

(e.g. 120s, 5m 30s, 4h)

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 ?

Custom Filter ?

Ports:

Client IP:

Server IP:

25

Note: Packet capture settings will be available for use immediately when submitted.

Cancel

Submit

**Step 4** [Table 2-2](#) describes the packet capture settings you can configure.

**Table 2-2 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"> <li>• <b>Run Capture Until File Size Limit Reached.</b> The packet capture runs until the file size limit is reached.</li> <li>• <b>Run Capture Until Time Elapsed Reaches.</b> 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.</li> </ul> <p><b>Note</b> 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"> <li>• <b>Run Capture Indefinitely.</b> The packet capture runs until you manually stop it.</li> </ul> <p><b>Note</b> 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 <b>tcpdump</b> command, such as <code>host 10.10.10.10 &amp;&amp; port 80</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Step 5** Click **Submit** to submit your changes on the page.

---

**Note**

AsyncOS uses the new packet capture settings after you submit them. In this case, you do not need to commit the changes.

---

## Working with Feature Keys

Occasionally, Cisco IronPort Customer Support may provide a key to enable specific functionality on your system.

On the main Security Management appliance, choose **Management Appliance > System Administration > Feature Keys** on the GUI (or the **featurekey** command from the command line prompt) to enter the key and enable the associated functionality.

Keys are specific to the serial number of your appliance and specific to the feature that you enable. You cannot reuse a key from one system on another system. If you incorrectly enter a key, an error message is generated.

Two pages provide feature keys functionality: the Feature Keys page and the Feature Key Settings page.

## Feature Keys Page

Log in to the Security Management appliance, and select **Management Appliance > System Administration > Feature Keys**. Use the Feature Keys page to perform the following tasks:

- View all active feature keys for the appliance.
- View any feature keys that are pending activation.
- Search for new keys that have been issued.
- Install feature keys.

The Feature Keys for Serial Number: <Serial Number> section lists the enabled features for the appliance. The Pending Activation section lists feature keys that have been issued for the appliance but have not yet been activated. By default, the

appliance periodically checks for new keys. You can change the appliance configuration to modify this behavior. In addition, you can click the **Check for New Keys** button to refresh the list of pending keys.

**Figure 2-11 Feature Keys Page**

### Feature Keys

| Feature Keys for Serial Number: 005056040102-vmware |        |                |                          |
|-----------------------------------------------------|--------|----------------|--------------------------|
| Description                                         | Status | Time Remaining | Expiration Date          |
| Centralized Reporting                               | Active | 29 days        | Sat Dec 15 16:15:50 2007 |
| Centralized Tracking                                | Active | 29 days        | Sat Dec 15 16:16:04 2007 |
| Centralized Spam Quarantine                         | Active | 29 days        | Sat Dec 15 16:16:17 2007 |
| Incoming Mail Handling                              | Active | 29 days        | Sat Dec 15 16:15:23 2007 |

| Pending Activation                      |  |
|-----------------------------------------|--|
| No feature key activations are pending. |  |

[Check for New Keys](#)

| Feature Activation |                      |
|--------------------|----------------------|
| Feature Key:       | <input type="text"/> |

[Submit Key](#)

To add a new feature key manually, paste or enter the key into the Feature Key field and click **Submit Key**. An error message appears if the feature is not added (for example, if the key is incorrect); otherwise, the feature key is added to the list.

To activate a new feature key from the Pending Activation list, select the key (select the Select check box) and click **Activate Selected Keys**.

You can configure your appliance to automatically download and install new keys as they are issued. In this case, the Pending Activation list is always empty.

## Feature Key Settings Page

Use the **Management Appliance > System Administration > Feature Key Settings** page to control whether the appliance checks for and downloads new feature keys, and whether or not the keys are automatically activated.

**Figure 2-12 Feature Key Settings Page**

### Feature Key Settings

| Feature Key Settings                 |                                                                                                                                                     |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Automatic Serving of Feature Keys: ? | <input checked="" type="checkbox"/> Check for and Download Automatically<br><input checked="" type="checkbox"/> Activate Feature Keys Automatically |

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

## Expired Feature Keys

If the feature key for the feature you are trying to access has expired, contact your Cisco representative or other customer support organization.

## SMA Compatibility Matrix

This section describes the compatibility between AsyncOS 7.7 for the Security Management appliance and the various AsyncOS releases for the Email Security appliance and the Web Security appliance. Additionally, it includes a table of supported Configuration file versions.



**Note**

(For Deployments with Web Security appliances) The Web Security appliance maintains backward compatibility of its configuration data for up to two previous major versions. It is important to remember though, that any upgrade may affect Security Management appliance functionality depending on what the software versions are on the source and destination appliances.

**Table 2-3      Security Management Appliance Compatibility with the Email Security Appliance**

| Version | Reporting  | Tracking   | SafeList/<br>BlockedList | ISQ     |
|---------|------------|------------|--------------------------|---------|
| ESA 6.3 | No Support | No Support | No Support               | Support |
| ESA 6.4 | Support    | Support    | Support                  | Support |
| ESA 6.5 | Support    | Support    | Support                  | Support |
| ESA 7.0 | Support    | Support    | Support                  | Support |
| ESA 7.1 | Support    | Support    | Support                  | Support |
| ESA 7.5 | Support    | Support    | Support                  | Support |

**Table 2-4 Security Management Appliance Compatibility with the Web Security Appliance**

| Version | Centralized Reporting and Tracking | ICCM Publish <sup>a</sup>                   | Advanced File Publish to the Web Security appliance (versions 5.7, 6.3, and 7.1) |
|---------|------------------------------------|---------------------------------------------|----------------------------------------------------------------------------------|
| WSA 5.6 | Feature not Available              | No support                                  | No support                                                                       |
| WSA 5.7 | Feature not Available              | Support on 5.7 Configuration Master         | Configuration file version must match target WSA version.                        |
| WSA 6.0 | Feature not Available              | No support                                  | No support                                                                       |
| WSA 6.3 | Feature not Available              | Support on 5.7 and 6.3 Configuration Master | Configuration file version must match target WSA version.                        |
| WSA 7.0 | Feature not Available              | Support on 6.3 Configuration Master         | Configuration file version must match target WSA version.                        |
| WSA 7.1 | Support                            | Support on 6.3 and 7.1 Configuration Master | Configuration file version must exactly match target WSA version.                |

- a. For ICCM Publish and Advanced File Publish rows in the table, the destination for the publish is a Web Security appliance.

**Table 2-5 (Deployments with WSAs Only) Configuration Master Compatibility**

| Target Configuration Master version: | Source Configuration Master version: | Source Configuration file from Web Security appliance version: |
|--------------------------------------|--------------------------------------|----------------------------------------------------------------|
| 5.7                                  | Not applicable                       | Web Security appliance 5.7                                     |
| 6.3                                  | Configuration Master 5.7             | Web Security appliance 6.3                                     |
| 7.1                                  | Configuration Master 6.3             | Web Security appliance 7.1                                     |







# CHAPTER 3

## Appliance Configuration

---

This chapter contains the following sections:

- [Appliance Configuration Overview, page 3-1](#)
- [Enabling Services on the Security Management Appliance, page 3-2](#)
- [Adding Managed Appliances, page 3-10](#)
- [Editing and Deleting Managed Appliances, page 3-14](#)
- [About Reports, page 3-16](#)

## Appliance Configuration Overview

After you run the System Setup Wizard on the Security Management appliance, you need to configure your Security Management appliance and your other Cisco IronPort appliances so that they can communicate.

To configure the Cisco IronPort appliances:

- 
- Step 1 Web Security appliance.** Configure networking, authorization, and security services, and configure and test policies. See the *Cisco IronPort AsyncOS for Web User Guide*.
- Step 2 Security Management appliance.** Enable management services. You need to enable the services on the Security Management appliance that manages your other Cisco IronPort appliances. You can enable one or more of the following services:
- Centralized reporting for Email and Web Security appliances

- Centralized tracking for Email appliances
- (Email) Cisco IronPort Spam Quarantine
- (Web) Cisco IronPort Centralized Configuration Manager

See the [“Enabling Services on the Security Management Appliance”](#) section on page 3-2.



#### Note

Counters were added for the Web Security appliance to report on the number of Web events happening on that appliance. On the Email Security appliance, counters were added to report on the number of Email events happening. Both Email and Web counters are now centralized on Security Management appliance at **Management Appliance > Centralized Services**. Both Email and Web counters share the Centralized Reporting Disk Space on Security Management appliance. If you only turn on Centralized Reporting, Email counters use all of the space. Conversely, if you only turn on Centralized Web Reporting, Web counters use all the disk space. If you turn on both, Email and Web reporting share the space and space is allocated on a first come basis. At this time there is no way to share the Centralized Reporting Disk Space to Email and Web categories.

- Step 3 Security Management appliance.** Add the Email Security appliances and Web Security appliances that you want to manage. On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances** to add Cisco IronPort appliances. See the [“Adding Managed Appliances”](#) section on page 3-10.
- Step 4 Email Security appliances.** Configure the monitoring and security services on the Web Security appliances and Email Security appliances that you want to manage. See [Chapter 9, “Monitoring System Status.”](#)

## Enabling Services on the Security Management Appliance

Before you can use the Security Management appliance to manage the Email Security appliances and Web Security appliances, you need to enable the appropriate services on the Security Management appliance.

Before you can use a Security Management appliance for centralized reporting and centralized tracking or as an external Cisco IronPort Spam Quarantine, you need to configure the monitoring services on the Email Security appliances.

**Note**

After you enable the services on the Security Management appliance, you need to add the appropriate Cisco IronPort appliances as managed appliances, if you have not done so already. For more information, see the [“Adding Managed Appliances” section on page 3-10](#).

To enable either Email or Web Security services on the Security Management appliance, see the following sections:

- [Enabling and Disabling Centralized Email Reporting on a Security Management Appliance, page 3-3](#)
- [Enabling and Disabling Centralized Web Reporting on a Security Management Appliance, page 3-5](#)
- [Enabling and Disabling Centralized Email Tracking on a Security Management Appliance, page 3-6](#)

## Enabling and Disabling Centralized Email Reporting on a Security Management Appliance

**Note**

Before enabling centralized email reporting, ensure that sufficient disk space is allocated to that service. See the [“Managing Disk Usage” section on page 12-115](#). Once you have enabled email reporting on the Security Management appliance, you can use monitoring services to run reports on email traffic, track message routing, and deliver suspect and spam messages to an external Cisco IronPort Spam Quarantine. For more information on how to configure monitoring services for the Email Security appliances, see *Cisco IronPort AsyncOS for Email User Guide*. For more information on monitoring services on the Security Management appliance, see [Chapter 9, “Monitoring System Status.”](#)

To enable centralized email reporting on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Centralized Reporting**.
  - Step 2** In the Email Reporting Service section, click **Enable**.
  - Step 3** If you are enabling centralized email reporting for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.  
The Centralized Reporting page appears.
  - Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- Once you have enabled centralized email reporting, you can create email reporting groups of managed Email Security appliances. See the [“Creating Email Reporting Groups” section on page 4-4](#). For more information about using centralized email reporting, see [Chapter 4, “Using Centralized Email Reporting.”](#)
- 

## Disabling Centralized Email Reporting

To disable centralized email reporting on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Centralized Reporting**.
  - Step 2** In the Reporting Services section click **Edit Settings**.
  - Step 3** Uncheck the **Enable Centralized Reporting Service** check box.
  - Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
-

# Enabling and Disabling Centralized Web Reporting on a Security Management Appliance



## Note

Before enabling centralized web reporting, ensure that sufficient disk space is allocated to that service. See the [“Managing Disk Usage” section on page 12-115](#).

Once you have enabled web reporting on the Security Management appliance, you can view and monitor services as well as run reports on web traffic. For more information on how to configure monitoring services for the Email Security appliances, see the *Cisco IronPort AsyncOS for Security Management User Guide*. For more information on monitoring services on the Security Management appliance, see [Chapter 9, “Monitoring System Status.”](#)

To enable centralized web reporting on a Security Management appliance:

- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.
- Step 2** In the Web Reporting Service section, click **Enable**.
- Step 3** If you are enabling centralized web reporting for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**. The Centralized Web Reporting page appears.
- Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.

Once you have enabled web centralized reporting, you can add web appliances from the Security Management appliance page, or allocate disk space appropriately from the Disk Management page. Additionally, you can configure web reporting to show or anonymize user names and roles in web reports. For more information on configuring web reports, see the [“Configuring Centralized Web Reporting” section on page 5-3](#).

For more information about these topics, see the [“Adding Managed Appliances” section on page 3-10](#), or the [“Managing Disk Usage” section on page 12-115](#).

## Disabling Centralized Web Reporting

To disable centralized web reporting on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.
  - Step 2** Click **Edit Settings**.
  - Step 3** Uncheck the **Enable Centralized Reporting Service** check box in the Web Reporting Service section.
  - Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- 

## Enabling and Disabling Centralized Email Tracking on a Security Management Appliance

Once you have enabled email message tracking on the Security Management appliance, you can use monitoring services to run reports on email traffic, track message routing, and deliver suspect and spam messages to an external Cisco IronPort Spam Quarantine. For more information on how to configure monitoring services for the Email Security appliances, see the *Cisco IronPort AsyncOS for Email User Guide*. For more information on monitoring services on the Security Management appliance, see [Chapter 9, “Monitoring System Status.”](#)

To enable centralized email tracking on a Security Management appliance:

- 
- Step 1** On the Security Management appliance:
    - a.** Choose **Management Appliance > Centralized Services > Email > Centralized Message Tracking**.
    - b.** In the Message Tracking Service section, click **Enable**.
    - c.** If you are enabling centralized email tracking for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.

The Centralized Message Tracking page appears. If centralized email tracking is enabled, 'Enable' appears in the right column of the Message Tracking Service box.

- d. **Submit** and commit your changes on the Security Management appliance.

**Step 2** On the Email Security appliance:

- a. If you want to be able to search for and log the names of attachments to email messages:

Make sure you have at least one incoming content filter or other body scanning feature configured and enabled on the Email Security appliance. For information about content filters and body scanning, see *Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*. (This feature was introduced in AsyncOS release 7.5.)

- b. In **Security Services > Message Tracking**, click **Edit Settings**, then select **Centralized Tracking**.

- c. Submit and commit your changes on the Email Security appliance.

For more information about using centralized tracking, see [Chapter 6, "Tracking Email Messages."](#)

## Disabling Centralized Email Tracking

To disable centralized email tracking on a Security Management appliance:

**Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Centralized Message Tracking**.

**Step 2** Click **Edit Settings**.

**Step 3** Uncheck the **Enable Centralized Message Tracking Service** check box.

**Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.

# Enabling and Disabling the Cisco IronPort Spam Quarantine on a Security Management Appliance



## Note

Once you have enabled the Cisco IronPort Spam Quarantine on the Security Management appliance, you can use monitoring services to run reports on email traffic, track message routing, and deliver suspect and spam messages to an external Cisco IronPort Spam Quarantine. For more information on how to configure monitoring services for the Email Security appliances, see *Cisco IronPort AsyncOS for Email User Guide*. For more information on monitoring services on the Security Management appliance, see [Chapter 9, “Monitoring System Status.”](#)

To enable the Cisco IronPort Spam Quarantine on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Spam Quarantine**.  
The Spam Quarantine page appears.
  - Step 2** Click **Enable**.
  - Step 3** If you are enabling the Cisco IronPort Spam Quarantine for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.  
The Edit Cisco IronPort Spam Quarantine page appears.
  - Step 4** (Optional) Edit the Spam Quarantine settings and configure access to the quarantine. For more information, see the [“Configuring Cisco IronPort Spam Quarantine Settings”](#) section on page 7-3.
  - Step 5** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
-



## Disabling the Cisco IronPort Spam Quarantine

To disable the Cisco IronPort Spam Quarantine on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Spam Quarantine**.
- The Spam Quarantine page appears.
- Step 2** Click **Edit Settings** in the Cisco IronPort Spam Quarantine Settings section.
- Step 3** Uncheck the **Enable Cisco IronPort Spam Quarantine** check box.
- Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- 

## Enabling and Disabling the Centralized Configuration Manager on a Security Management Appliance

To enable the Cisco IronPort Centralized Configuration Manager on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Configuration Manager**.
- Step 2** On the Centralized Configuration Manager page, click **Enable**.
- Step 3** If you are enabling the Cisco IronPort Centralized Configuration Manager for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.
- The Centralized Configuration Manager page appears and shows that the service is enabled.
- Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
-

## Disabling the Cisco IronPort Centralized Configuration Manager

To disable the Cisco IronPort Centralized Configuration Manager on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Configuration Manager**.
  - Step 2** Click **Edit Settings**.
  - Step 3** Uncheck the **Enable Centralized Configuration Manager Service** check box.
  - Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- 

## Adding Managed Appliances

After you enable monitoring services on the Security Management appliance, you need to add connection information for the appliances that it manages. You can connect supported Email and Web Security appliances, as defined in the [SMA Compatibility Matrix, page 2-32](#).

When you add a remote appliance, the Security Management appliance compares the product name of the remote appliance with the type of appliance you are adding. For example, you add an appliance using the Add Web Security appliance page, the Security Management appliance checks the product name of the remote appliance to make sure that it is a Web Security appliance and not an Email Security appliance. The Security Management appliance will also check the monitoring services on the remote appliances to make sure that they are correctly configured and compatible.

To add managed appliances to a Security Management appliance perform the following steps:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.

The Security Appliances page appears.

**Figure 3-1 The Security Appliances Page****Security Appliances**

| Centralized Service Status   |                           |
|------------------------------|---------------------------|
| Configuration Manager (Web): | Enabled, using 0 licenses |
| Spam Quarantine:             | Service disabled          |
| Reporting:                   | Enabled, using 0 licenses |
| Tracking:                    | Enabled, using 0 licenses |

| Security Appliances                    |  |
|----------------------------------------|--|
| <b>Email</b>                           |  |
| <a href="#">Add Email Appliance...</a> |  |
| No appliances have been added.         |  |
| <b>Web</b>                             |  |
| <a href="#">Add Web Appliance...</a>   |  |
| No appliances have been added.         |  |

**Step 2** Click **Add Email Appliance** button to display the Add Email Security Appliance page.

**Figure 3-2 The Add Email Security Appliance Page****Add Email Security Appliance**

| Email Security Appliance Settings |                                                                                                                                                                                                                                                 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Name:                   | <input type="text"/>                                                                                                                                                                                                                            |
| IP Address: ?                     | <input type="text"/>                                                                                                                                                                                                                            |
| ESA Centralized Services:         | <input checked="" type="checkbox"/> Spam Quarantine<br><input checked="" type="checkbox"/> Centralized Reporting<br><input checked="" type="checkbox"/> Centralized Message Tracking                                                            |
| Connection Status:                | Not established.<br><i>Establish an SSH connection for synchronization of the Spam Quarantine's Safelist/Blocklist, Centralized Reporting, and Message Tracking.</i><br><a href="#">Establish Connection...</a> <a href="#">Test Connection</a> |

or

Click **Add Web Appliance** button to display the Add Web Security Appliance page.

**Figure 3-3 The Add Web Security Appliance Page****Add Web Security Appliance**

| Web Security Appliance Settings |                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Name:                 | <input type="text"/>                                                                                                                                                                            |
| IP Address:                     | <input type="text"/>                                                                                                                                                                            |
| WSA Centralized Services:       | <input checked="" type="checkbox"/> Centralized Configuration Manager<br><input checked="" type="checkbox"/> Centralized Reporting                                                              |
| Connection Status:              | Not established.<br><i>Establish an SSH connection for Centralized Web Services.</i><br><input type="button" value="Establish Connection..."/> <input type="button" value="Test Connection"/>   |
| Assign Configuration Master: ?  | <i>More assignment options may be enabled once an SSH connection is established.</i><br><input checked="" type="radio"/> Not Assigned<br><input type="radio"/> 5.7<br><input type="radio"/> 7.1 |

- Step 3** In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Cisco IronPort appliance.



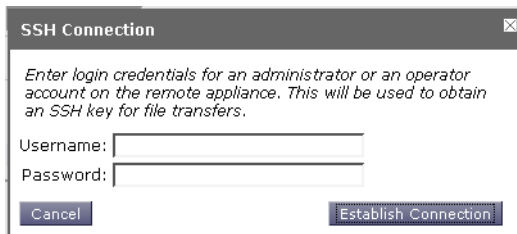
**Note** A DNS name may be entered in the IP Address text field, however, it will be immediately resolved to an IP address when you click **Submit**.

- Step 4** Select the services that you want to use when managing the Cisco IronPort appliance.



**Note** You can select a service only if you have enabled it on the Security Management appliance. For more information, see the [“Enabling Services on the Security Management Appliance”](#) section on page 3-2.

- Step 5** Click **Establish Connection**.  
The SSH Connection dialog box appears.

**Figure 3-4 The SSH Connection Dialog Box**

- Step 6** In the Username and Password text fields, type in the login credentials for an administrator account on the Cisco IronPort appliance.



**Note** You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

- Step 7** Click **Establish Connection** to establish the connection for the monitoring services.
- Step 8** Click **Test Connection** to verify that the monitoring services on the remote appliance have been correctly configured and are compatible.
- Step 9** If you are adding a Web Security appliance, choose the Configuration Master to which you want to assign the appliance.

Each Configuration Master contains the configuration for a version of the Web Security appliances. The Security Management appliance can publish a Configuration Master only to a Web Security appliance that is running a compatible version of AsyncOS (for example, if the Web Security appliance is running AsyncOS 6.3, then choose 6.3.0 as the Configuration Master). You can also assign the Web Security appliance later by choosing **Web > Utilities > Configuration Masters** (see the [“Associating Web Security Appliances to Configuration Masters”](#) section on page 8-8).

For more information about Configuration Masters and managing Web Security appliances, see [Chapter 8, “Managing Web Security Appliances.”](#)

- Step 10** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.

The Security Appliances page shows the managed appliances that you have added. Check marks indicate the enabled services, and the Connection Established? column shows whether or not the connection for monitoring services is properly configured.

**Figure 3-5 A Managed Appliance on the Security Appliances Page**

|                      |  |         |  |                       |  |
|----------------------|--|---------|--|-----------------------|--|
| Management Appliance |  |         |  |                       |  |
| Email Web            |  |         |  |                       |  |
| Centralized Services |  | Network |  | System Administration |  |

|                                        |  |                           |  |  |  |
|----------------------------------------|--|---------------------------|--|--|--|
| Security Appliances                    |  |                           |  |  |  |
| Centralized Service Status             |  |                           |  |  |  |
| Centralized Web Configuration Manager: |  | Enabled, using 0 licenses |  |  |  |
| Centralized Web Reporting:             |  | Enabled, using 2 licenses |  |  |  |
| Spam Quarantine:                       |  | Service disabled          |  |  |  |
| Centralized Email Reporting:           |  | Service disabled          |  |  |  |
| Centralized Email Message Tracking:    |  | Service disabled          |  |  |  |

| Security Appliances                              |              |                       |           |                         |        |
|--------------------------------------------------|--------------|-----------------------|-----------|-------------------------|--------|
| Email                                            |              |                       |           |                         |        |
| No centralized services are currently available. |              |                       |           |                         |        |
| Web                                              |              |                       |           |                         |        |
| Add Web Appliance...                             |              |                       |           |                         |        |
| Appliance Name ▲                                 | IP Address   | Services              |           | Connection Established? | Delete |
|                                                  |              | Configuration Manager | Reporting |                         |        |
| vm-03                                            | 10.92.152.89 | ✓                     | ✓         | Yes                     |        |
| wsa-04                                           | 10.92.152.90 | ✓                     | ✓         | Yes                     |        |

Key: ✓ Selected

## Editing and Deleting Managed Appliances

After you add a managed appliance to the Security Management appliance, you may need to edit or delete the configuration.

### Editing a Managed Appliance

To edit the configuration of a managed appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 2** In the Security Appliance section, click on the name of the appliance you want to edit.
- Step 3** Make the necessary changes to the appliance configuration.
- For example, select or clear check boxes for monitoring services, reconfigure file transfer access, or change the IP address.



**Note** Changing the IP address of a managed appliance can cause several issues to occur. If you change the IP address of a Web Security appliance, the publish history for the appliance will be lost, and publishing errors will occur if the Web Security appliance is currently selected for a scheduled publish job. (This does not affect scheduled publish jobs that are set to use all assigned appliances.) If you change the IP address of an Email Security appliance, the tracking availability data for the appliance will be lost.

---

- Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- 

## Deleting a Managed Appliance

To remove a Cisco IronPort appliance from the list of managed appliances:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 2** In the Security Appliances section, and click the trash can icon in the row for the managed appliance that you want to delete.
- Step 3** In the confirmation dialog box, click **Delete**.
- Step 4** Click **Submit** and then click **Commit Changes** to commit your changes.
-

# About Reports

On all of the Cisco IronPort appliances, there are basic concepts, settings and pages that are common to the Email Security appliance, Web Security appliance, and Security Management appliance. Reporting information includes:

- [“Reporting Options” section on page 3-16](#)
- [“How the Security Appliance Gathers Data for Reports” section on page 3-16](#)
- [“Interactive Report Pages” section on page 3-17](#)
- [“Choosing a Time Range for Interactive Reports” section on page 3-18](#)
- [“Reporting Filters on the Security Management Appliance” section on page 3-19](#)
- [“Printing and Exporting Report Data” section on page 3-20](#)

## Reporting Options

You have many options for viewing and saving data:

- View and customize interactive report pages and generate a PDF of the report you are viewing
- Generate a PDF or CSV file for any of several predefined report types at any time on demand
- Schedule automated creation of predefined PDF or CSV reports at times that you specify
- Have scheduled or on-demand reports emailed to recipients of your choice
- View archived copies of scheduled and on-demand reports until they are purged from the system

## How the Security Appliance Gathers Data for Reports

The Security Management appliance pulls data for all reports from all managed appliances approximately every 15 minutes and aggregates the data from these appliances. Depending on your appliance, it may take awhile for a particular message to be included in the reporting data on the Security Management appliance. Check the **System Status** page for information on your data.



**Note**

When gathering data for reports, the Security Management appliance applies the time stamp from the information that was set when you configured the time settings on the Security Management appliance. For information on setting the time on your Security Management appliance, see the [“Configuring the System Time” section on page 12-98](#).

## How Reporting Data is Stored

All of the appliances store reporting data. [Table 3-1](#) shows what time periods that each appliance stores data.

**Table 3-1**      *Reporting Data Storage on the Email and Web Security Appliances*

|                                                      | Minute | Hourly | Daily | Weekly | Monthly | Yearly |
|------------------------------------------------------|--------|--------|-------|--------|---------|--------|
| <b>Local Reporting on C-Series or S-Series</b>       | •      | •      | •     | •      | •       |        |
| <b>Centralized Reporting on C-Series or S-Series</b> | •      | •      | •     | •      |         |        |
| <b>M-Series</b>                                      |        | •      | •     | •      | •       | •      |

## Interactive Report Pages

All of the reports pages on the appliances are interactive report pages. This allows you to monitor information on one or all of the managed Email and Web Security appliances in your system. With the interactive report pages, you can view centralized tracking and reporting data for different time ranges, and specify what column types you want to view on each page.

For more information on interactive report pages for each appliance, see:

- [Using the Email Reporting Tab, page 4-6](#)
- [Interactive Report Pages for the Web Security Appliance, page 5-10](#)

## Choosing a Time Range for Interactive Reports

Most interactive report pages allow you to choose a Time Range for the data to include. The time range that you select is used throughout all of the report pages until you select a different value in the Time Range menu.

Available Time Range options differ by appliance and differ for Email and Web reporting on the Security Management appliance:

**Table 3-2** *Time Range Options for Reports*

| Option                         | Description                                                                                         | SMA<br>Email<br>reports | ESA | SMA<br>Web<br>reports | WSA |
|--------------------------------|-----------------------------------------------------------------------------------------------------|-------------------------|-----|-----------------------|-----|
| <b>Hour</b>                    | The previous 60 minutes, plus up to 5 additional minutes                                            |                         | •   |                       | •   |
| <b>Day</b>                     | The previous 24 hours                                                                               | •                       | •   | •                     | •   |
| <b>Week</b>                    | The previous seven days, including the elapsed hours of the current day                             | •                       | •   | •                     | •   |
| <b>30 days</b>                 | The previous 30 days, including the elapsed hours of the current day                                | •                       | •   | •                     | •   |
| <b>90 days</b>                 | The previous 90 days, including the elapsed hours of the current day                                | •                       | •   | •                     |     |
| <b>Year</b>                    | The last 12 months plus the elapsed days of the current month                                       | •                       |     |                       |     |
| <b>Yesterday</b>               | 24 hours (00:00 to 23:59) of the previous day, using the time zone defined on the appliance         | •                       | •   | •                     | •   |
| <b>Previous Calendar Month</b> | 00:00 of the first day of the month to 23:59 of the last day of the month                           | •                       | •   | •                     |     |
| <b>Custom Range</b>            | The time range that you specify.<br><br>Select this option to choose start and end dates and times. | •                       | •   | •                     | •   |

**Note**

Time ranges on interactive report pages are displayed as a Greenwich Mean Time (GMT) offset. For example, Pacific time is GMT + 7 hours (GMT + 07:00).

## Reporting Filters on the Security Management Appliance

AsyncOS provides reporting filters that allow you to restrict the aggregation of data in reports that cover the previous year (Last Year reports). You can use these filters if the performance of aggregated reporting decreases due to a large number of unique entries over the course of a month. These filters can restrict detailed, individual IP, domain, or user data in reports. Overview reports and summary information remain available for all reports.

You can enable one or more of the reporting filters using the **reportingconfig -> filters** menu in the CLI. The changes must be committed to take effect.

- **IP Connection Level Detail.** Enabling this filter prevents the Security Management appliance from recording information about individual IP addresses. This filter is appropriate for systems that process a large number of incoming IP addresses due to attacks.

This filter affects the following Last Year reports:

- Sender Profile for Incoming Mail
- IP Addresses for Incoming Mail
- IP Addresses for Outgoing Senders
- **User Detail.** Enabling this filter prevents the Security Management appliance from recording information about individual users sending and receiving mail and the content filters that are applied to the users' mail. This filter is appropriate for appliances that process mail for millions of internal users or if the system does not validate recipient addresses.

This filter affects the following Last Year reports:

- Internal Users
- Internal User Details
- IP Addresses for Outgoing Senders
- Content Filters

- **Mail Traffic Detail.** Enabling this filter prevents the Security Management appliance from recording information about individual domains and networks that the appliances monitor. This filter is appropriate when the number of valid incoming or outgoing domains is measured in the tens of millions.

This filter affects the following Last Year reports:

- Domains for Incoming Mail
- Sender Profile for Incoming Mail
- Internal User Details
- Domains for Outgoing Senders



#### Note

To view up-to-the-minute reporting data for the preceding hour, you must log in to an individual appliance and view the data there.

## Printing and Exporting Report Data

You can generate a printer-friendly formatted PDF version of any of the report pages by clicking the Printable PDF link at the top-right of the page.

Additionally, you can export graph and other raw data to comma-separated values (CSV) format by clicking the **Export** link. Most reports allow scheduling of CSV formatting. However, you cannot schedule an extended report with a CSV format.

You can schedule a PDF or CSV report with a specific locale for that individual report. The language drop-down menu on the Scheduled Reports page allows you to view or schedule a PDF report in the current selected locale and language.



#### 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.

In some cases, some of the report pages contain several unique sub-reports that can be accessed from the top-level page. For example, the Incoming Mail report page on the Email Security appliance allows you to see information for individual IP Addresses, Domains and Network Owners. Each of these sub-pages are accessed from the Incoming Mail report page.

Results for each of these sub-report pages are generated on one consolidated report when you click on the Printable PDF link at the top-right of the top-level page; in this case the Incoming Mail report page.


**Note**

The only exception to printing to PDF is when you are using the [Web Tracking Page](#). From the [Web Tracking Page](#) you can only print using the Printable Download link. From this link you can choose to print a PDF of: the current page, up to 10,000 transactions, or print all data to a CSV file.

## Exporting Report Data

Export links are visible on most of the reporting pages on the Security Management appliance. This link will export raw data to a comma-separated values (CSV) file, that you can access and manipulate using database applications such as, Microsoft Excel.

The exported CSV data will display all message tracking and reporting data in GMT regardless of what is set on the Security Management 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.

The following example is an entry from a raw data export of the Anti-Malware category report, where Pacific Daylight Time (PDT) is displayed as GMT - 7 hours:

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
Transactions Monitored, Transactions Blocked, Transactions Detected
1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59
GMT, Adware, 525, 2100, 2625
```

**Table 3-3 Viewing Raw Data Entries**

| Category Header | Value                | Description                                       |
|-----------------|----------------------|---------------------------------------------------|
| Begin Timestamp | 1159772400.0         | Query start time in number of seconds from epoch. |
| End Timestamp   | 1159858799.0         | Query end time in number of seconds from epoch.   |
| Begin Date      | 2006-10-02 07:00 GMT | Date the query began.                             |

**Table 3-3** *Viewing Raw Data Entries (continued)*

| Category Header        | Value                | Description                                                                                           |
|------------------------|----------------------|-------------------------------------------------------------------------------------------------------|
| End Date               | 2006-10-03 06:59 GMT | Date the query ended.                                                                                 |
| Name                   | Adware               | Name of the malware category.                                                                         |
| Transactions Monitored | 525                  | Number of transactions monitored.                                                                     |
| Transactions Blocked   | 2100                 | Number of transactions blocked.                                                                       |
| Transactions Detected  | 2625                 | Total number of transactions:<br>Number of transactions detected +<br>Number of transactions blocked. |

**Note**

Category headers are different for each type of report.

If you export localized CSV data, the headings may not be rendered properly in some browsers. This occurs because some browsers may not use the proper character set for the localized text. To work around this problem, you can save the file to your local machine, and open the file on any web browser using **File > Open**. When you open the file, select the character set to display the localized text.



## CHAPTER 4

# Using Centralized Email Reporting

---

This chapter contains the following sections:

- [Reporting Overview, page 4-1](#)
- [Getting Started with Email Reporting, page 4-2](#)
- [Using the Email Reporting Tab, page 4-6](#)
- [Understanding the Email Reporting Pages, page 4-11](#)
- [About Scheduled and On-Demand Reports, page 4-66](#)
- [Generating Reports On Demand, page 4-73](#)
- [Scheduled Reports, page 4-75](#)
- [Archived Reports, page 4-78](#)

## Reporting Overview

The Email reporting functionality aggregates information from individual or multiple Email Security appliances so that you can monitor your email traffic patterns and security risks. You can run reports in real-time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals. Reporting functionality also allows you to export raw data to a file.

The Centralized Email Reporting feature not only generates high-level reports, allowing you to understand what is happening on their network, but it also allows you to drill down and see traffic details for a particular domain, user, or category.

The Centralized Tracking feature allows you to track email messages that traverse multiple Email Security appliances.

## Getting Started with Email Reporting



### Note

Before you can view email reporting for the Email Security appliances, you must add and configure one or more Email Security appliances. For information on adding an Email Security appliance, see the [“Adding Managed Appliances” section on page 3-10](#); for information on configuring settings on the Email Security appliances, see the *Cisco IronPort AsyncOS for Email Security Configuration Guide*.

There are several ways that you can view email reporting data on the Security Management appliance. To get started on email reporting, use the following steps:

- To enable email reporting, see [Configuring Centralized Email Reporting, page 4-2](#)
- To create email reporting groups, see [Creating Email Reporting Groups, page 4-4](#)
- To view and understand the various interactive report pages, see [Understanding the Email Reporting Pages, page 4-11](#).
- To generate a report on demand, see [Generating Reports On Demand, page 4-73](#).
- To schedule reports to run automatically at intervals and times that you specify, see [Scheduled Reports, page 4-75](#).
- To view archived on-demand and scheduled reports, see [Archived Reports, page 4-78](#).

## Configuring Centralized Email Reporting

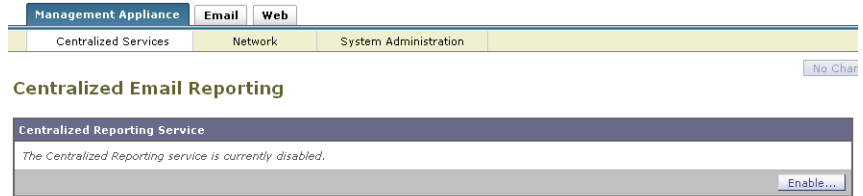
Before you use email reporting on the Security Management appliance, you must configure the Security Management appliance to enable all email reporting.

To configure the settings for centralized email reporting:



**Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Centralized Reporting**.

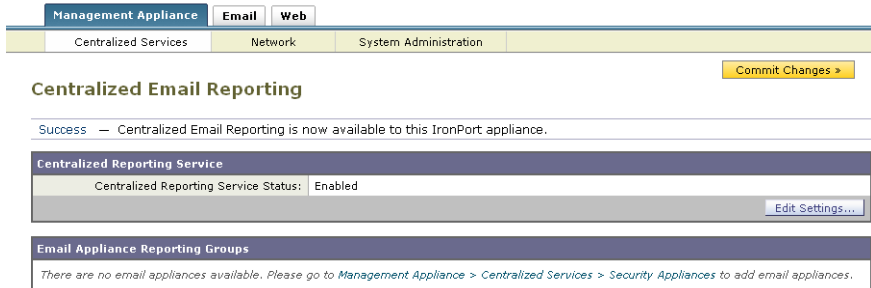
The Centralized Email Reporting page appears.



**Step 2** Click **Enable**.

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

The following window appears acknowledging that you have successfully enabled centralized reporting on the Security Management appliance.



Once you have enabled centralized reporting you can edit the settings.

**Step 3** Click **Edit Settings**.

**Step 4** The Edit Centralized Email Reporting Service Settings page appears.

Logged in as: **admin** on **esx16-sma01.qa**  
Options ▾ Help and Support ▾

|                      |         |                       |
|----------------------|---------|-----------------------|
| Management Appliance | Email   | Web                   |
| Centralized Services | Network | System Administration |

**Edit Centralized Email Reporting Service Settings** Commit Changes ▶

|                                                                                                          |
|----------------------------------------------------------------------------------------------------------|
| Centralized Reporting Service                                                                            |
| <input checked="" type="checkbox"/> <b>Enable Centralized Reporting Service</b>                          |
| <i>If you turn off this service you will not be able to use the Centralized Email Reporting feature.</i> |

Cancel Submit

**Step 5** Click the **Enable Centralized Reporting Services** checkbox.

The Email Security appliance only stores data if local reporting is used. If centralized reporting is enabled for the Email Security appliance then the Email Security appliance does NOT retain any reporting data except for System Capacity and System Status. If Centralized Email Reporting is not enabled, the only reports that are generated are System Status and System Capacity.

**Step 6** Click **Submit** to submit your changes, then click the **Commit Changes** to commit your changes on the appliance.



**Note**

If you have enabled email reporting on the appliance, and there is no disk space allocated for this action, centralized email reporting will not work until disk space is allocated. As long as the quota you are setting the Email Reporting and Tracking to is larger than the currently used disk space, you will not lose any reporting and tracking data. See the [“Managing Disk Usage” section on page 12-115](#), for more information.

## Creating Email Reporting Groups

You can create groups of Email Security appliances for which to view reporting data from the Security Management appliance.

## Adding Email Reporting Groups

To add an email reporting group, perform the following:

**Step 1** On the main Security Management appliance, choose **Management Appliance > Centralized Services > Centralized Reporting**.

**Step 2** Click **Add Group**.

The Add Email Reporting Group page appears.

**Figure 4-1** Add Email Reporting Group Page

### Add Email Reporting Group

**Step 3** Enter a unique name for the group.

The Email Security appliance list displays the Email Security appliances that you added to the Security Management appliance. Select the appliances that you want to add to the group.

The maximum number of groups that can be added is smaller than or equal to the maximum number of email appliances that can be connected.



**Note** If you added an Email Security appliance to the Security Management appliance, but you do not see it in the list, edit the configuration of the Email Security appliance so that the Security Management appliance is collecting reporting data from it.

**Step 4** Click **Add** to add the appliances to the Group Members list.

- Step 5** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.



**Note** Appliances may be part of more than one group.

## Editing and Deleting Email Reporting Groups

To edit or delete an email reporting group:

- Step 1** On the main Security Management appliance window, choose **Management Appliance > Centralized Services > Centralized Reporting**
- The Centralized Reporting page appears. From this page you can view the Email Security appliance reporting groups.
- Step 2** To delete a group, click the corresponding trash can icon next to the group you want to delete.
- or
- To edit a group, click the name of the group you want to edit.
- The **Edit Email Reporting Group** page appears. From this page you can edit the group.
- Step 3** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.

## Using the Email Reporting Tab

The **Email > Reporting** tab provides several options for viewing reporting data. This section describes each of the reporting pages under this tab, and explains the information displayed on each of the reporting pages.



**Note** For a summary of reporting options, see [Reporting Options, page 3-16](#).

**Table 4-1**      **Email Reporting Tab Details**

| Email Reporting Menu                          | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Email Reporting Overview Page</a> | <p>The Overview page provides a synopsis of the activity on your Cisco IronPort Email appliances. It includes graphs and summary tables for the incoming and outgoing messages.</p> <p>For more information, see the <a href="#">“Email Reporting Overview Page”</a> section on page 4-12.</p>                                                                                                                                                                                |
| <a href="#">Incoming Mail Page</a>            | <p>The Incoming Mail page provides interactive reporting on the real-time information for all remote hosts connecting to your managed Email Security appliances. You can gather information about the IP addresses, domains, and network owners (organizations) sending mail to your system.</p> <p>For more information, see the <a href="#">“Incoming Mail Page”</a> section on page 4-17.</p>                                                                              |
| <a href="#">Outgoing Destinations Page</a>    | <p>The Outgoing Destinations page provides information about the domains that your organization sends mail to. The top of the page includes graphs depicting the top destinations by outgoing threat messages and top destinations by outgoing clean messages. The bottom of the page displays a chart with columns sorted by total recipients (default setting).</p> <p>For more information, see the <a href="#">“Outgoing Destinations Page”</a> section on page 4-31.</p> |
| <a href="#">Outgoing Senders Page</a>         | <p>The Outgoing Senders page provides information about the quantity and type of mail being sent from IP addresses and domains in your network.</p> <p>For more information, see the <a href="#">“Outgoing Senders Page”</a> section on page 4-33.</p>                                                                                                                                                                                                                        |
| <a href="#">Internal Users Page</a>           | <p>The Internal Users provides information about the mail sent and received by your internal users <i>per email address</i>. A single user can have multiple email addresses. The email addresses are not combined in the report.</p> <p>For more information, see the <a href="#">“Internal Users Page”</a> section on page 4-36.</p>                                                                                                                                        |

**Table 4-1 Email Reporting Tab Details**

| Email Reporting Menu             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DLP Incident Summary Page</b> | <p>The DLP Incident Summary page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail.</p> <p>For more information, see the <a href="#">“DLP Incident Summary Page” section on page 4-40.</a></p>                                                                                                                                                                                                        |
| <b>Content Filters Page</b>      | <p>The Content Filters page shows information about the top incoming and outgoing content filter matches (which content filter had the most matching messages). This page also displays the data as both bar charts and listings. Using the Content Filters page, you can review your corporate policies on a per-content-filter or per-user basis.</p> <p>For more information, see the <a href="#">“Content Filters Page” section on page 4-43.</a></p>         |
| <b>Virus Types Page</b>          | <p>The Virus Types page provides an overview of the viruses that are sent to and from your network. The Virus Types page displays the viruses that have been detected by the virus scanning engines running on the Email Security appliances and are displayed on the Security Management appliance. Use this report to take action against a particular virus.</p> <p>For more information, see the <a href="#">“Virus Types Page” section on page 4-45.</a></p> |
| <b>TLS Connections Page</b>      | <p>The TLS Connections page 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.</p> <p>For more information, see the <a href="#">“TLS Connections Page” section on page 4-48.</a></p>                                                                                                                                                                        |
| <b>Outbreak Filters Page</b>     | <p>The Outbreak Filters page shows information about recent outbreaks and the messages quarantined by Outbreak Filters. Use this page to monitor your defense against virus attacks.</p> <p>For more information, see the <a href="#">“Outbreak Filters Page” section on page 4-51.</a></p>                                                                                                                                                                       |

**Table 4-1**      *Email Reporting Tab Details*

| Email Reporting Menu                   | Action                                                                                                                                                                                                                                                              |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">System Capacity Page</a>   | Allows you to view the overall workload that is sending reporting data to the Security Management appliance.<br>For more information, see the <a href="#">“System Capacity Page” section on page 4-55</a> .                                                         |
| <a href="#">Data Availability Page</a> | Allows you to get a glimpse of the impact of the reporting data on the Security Management appliance for each appliance.<br>For more information, see the <a href="#">“Data Availability Page” section on page 4-64</a> .                                           |
| <a href="#">Scheduled Reports</a>      | Allows you to schedule reports for a specified time range. For more information, see the <a href="#">“Scheduled Reports” section on page 4-75</a> .                                                                                                                 |
| <a href="#">Archived Reports</a>       | Allows you to view and manage archived reports. For more information, see the <a href="#">“Archived Reports” section on page 4-78</a> .<br>Also allows you to generate on-demand reports. See <a href="#">“Generating Reports On Demand” section on page 4-73</a> . |

## Viewing Interactive Reports

When looking at interactive report pages, you can customize your view by:

- **Specifying a time range.** For information, see the [“Choosing a Time Range for Interactive Reports” section on page 3-18](#).
- **Choosing the table columns to display.** Click the Columns link below a table to select columns to show or hide. For a description of each column, see the [“Interactive Columns for the Centralized Email Reporting Pages” section on page E-5](#).
- **Reordering table columns** by dragging and dropping them.
- **Clicking a column heading to sort the table** by the data in that column.
- **Filtering the data displayed.** For details, see the [“Reporting Filters on the Security Management Appliance” section on page 3-19](#).
- **Searching for specific information to include.** See [“Searching and the Interactive Report Pages” section on page 4-10](#).

**Note**

Not all interactive features are available for every report.

## Searching and the Interactive Report Pages

Many of the interactive email reporting pages include a **Search For:** drop-down menu.

The following picture shows the **Search For** drop-down menu.

Search for: Domain [v] [exact match] Search ?

For additional information, see: [Sender Groups report](#)

From the drop-down menu, you can search for several types of criteria, including the following:

- IP address
- Domain
- Network owner
- Internal user
- Destination domain
- Internal sender domain
- Internal sender IP address
- Incoming TLS domain
- Outgoing TLS domain

For most searches, choose whether to exactly match the search text or look for items starting with the entered text (for example, starts with “ex” will match “example.com”).

For IP address searches, the entered text is always interpreted as the beginning of up to four IP octets in dotted decimal format. For example, ‘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, enter all four octets. IP address searches also support Classless Inter-Domain Routing (CIDR) format (17.16.0.0/12).



## Reporting Filters for Report Pages

AsyncOS provides reporting filters that allow you to restrict the aggregation of data in reports that cover the previous year (Last Year reports). You can use these filters if the performance of aggregated reporting decreases due to a large number of unique entries over the course of a month. These filters can restrict detailed, individual IP, domain, or user data in reports. Overview reports and summary information remain available for all reports.

For more information on how to enable reporting filters, see [“Reporting Filters on the Security Management Appliance” section on page 3-19](#).

## Printing and Exporting Reports from Report Pages

See [Printing and Exporting Report Data, page 3-20](#).

## More Information about Reports and Report Pages

- [“Reporting Options” section on page 3-16](#)
- [“How the Security Appliance Gathers Data for Reports” section on page 3-16](#)

## Understanding the Email Reporting Pages

This section discusses the various report pages that are used by the Security Management appliance for Email Reporting.

They include:

- [Email Reporting Overview Page, page 4-12](#)
- [Incoming Mail Page, page 4-17](#)
- [Outgoing Destinations Page, page 4-31](#)
- [Outgoing Senders Page, page 4-33](#)
- [Internal Users Page, page 4-36](#)
- [DLP Incident Summary Page, page 4-40](#)

- [Content Filters Page, page 4-43](#)
- [Virus Types Page, page 4-45](#)
- [TLS Connections Page, page 4-48](#)
- [Outbreak Filters Page, page 4-51](#)
- [System Capacity Page, page 4-55](#)
- [Data Availability Page, page 4-64](#)

## Email Reporting Overview Page

The **Email > Reporting > Overview** page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Overview page includes graphs and summary tables for the incoming and outgoing messages.

To view the Overview page, perform the following steps:

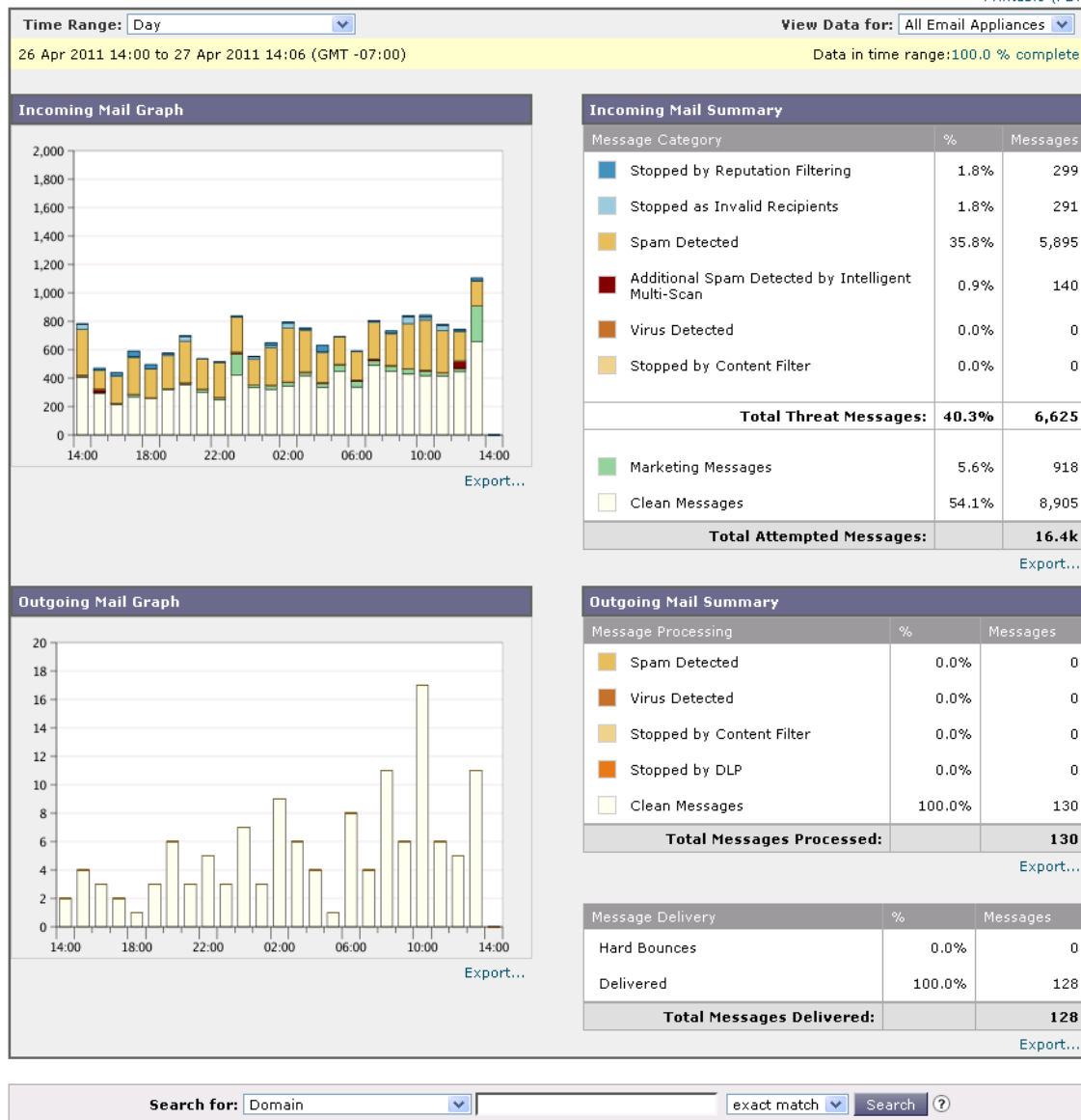
- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Email > Reporting > Overview**.

The Overview page appears.

[Figure 4-2](#) shows the Overview page.

Figure 4-2 The Email &gt; Reporting &gt; Overview Page

## Overview

[Printable \(PDF\)](#)

At a high level the **Overview** page shows you the incoming and outgoing mail graphs, and well as incoming and outgoing mail summaries.

The mail trend graphs provide a visual representation of the mail flow. You can use the mail trend graphs on this page to monitor the flow of all mail into and out of your appliances.



**Note**

It is important to remember that the Domain-Based Executive Summary Report, and the Executive Summary report are based on the [Email Reporting Overview Page](#). The Domain-Based Executive Summary report is limited to a group of specified domains. For information scheduling reports, see the “[Scheduled Reports](#)” section on page 4-75.

The following list explains the various sections on the **Overview** page:

**Table 4-2**      ***Details on the Email > Reporting > Overview Page***

| Section                      | Description                                                                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range</b>            | A drop-down list with options for choosing a time range to view. For more information, see the “ <a href="#">Choosing a Time Range for Interactive Reports</a> ” section on page 3-18.                                                                 |
| <b>Incoming Mail Graph</b>   | The Incoming Mail Graph displays a visual graph of the breakdown of incoming mail in real time.                                                                                                                                                        |
| <b>Outgoing Mail Graph</b>   | The Outgoing Mail graph displays a visual graph of the breakdown of outgoing mail on the appliance.                                                                                                                                                    |
| <b>Incoming Mail Summary</b> | The Incoming Mail Summary shows the percentages and the number of messages that were stopped by reputation filtering (SBRS), stopped as invalid recipient, spam detected, virus detected, and stopped by content filter, and those considered “clean.” |
| <b>Outgoing Mail Summary</b> | The Outgoing Mail Summary section includes information about the outgoing threat and clean messages. It also includes a breakdown of the delivered versus hard-bounced messages.                                                                       |

## How Incoming Mail Messages are Counted

AsyncOS counts incoming mail dependent on the number of recipients per message. For example, an incoming message from example.com sent to three recipients is counted as three messages coming from that sender.

Because the 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 IronPort Systems and is based on research of a large sampling of existing customer data.

## How Email Messages Are Categorized by the Appliances

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)
- Spam positive
- Virus positive
- Matching a content filter

Following these rules, 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 email 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.

## Categorizing Email Messages on Overview Page

Messages reported on the Overview page are categorized as follows:

**Table 4-3**      ***Email Categories on Overview Page***

| Category                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Stopped by Reputation Filtering</b> | <p>All connections blocked by HAT policies multiplied by a fixed multiplier (see the <a href="#">“How Incoming Mail Messages are Counted” section on page 4-15</a>) plus all recipients blocked by recipient throttling.</p> <p>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 limited due to load.</p> |
| <b>Invalid Recipients</b>              | All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.                                                                                                                                                                                                                                                                                                                                             |
| <b>Spam Messages Detected</b>          | The total count of messages detected by the anti-spam scanning engine as positive or suspect. Additionally, messages that are both spam and virus positive.                                                                                                                                                                                                                                                                        |
| <b>Virus Messages Detected</b>         | The total count and percentage of messages detected as virus positive and not also spam.                                                                                                                                                                                                                                                                                                                                           |
| <b>Stopped by Content Filter</b>       | The total count of messages that were stopped by a content filter.                                                                                                                                                                                                                                                                                                                                                                 |

**Table 4-3**      **Email Categories on Overview Page**

| Category                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Marketing Messages      | The total count and percentage of messages detected as unwanted marketing messages. This list item appears on the page only if marketing data are present in the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Clean Messages Accepted | <p>This category is mail that is accepted and deemed to be virus and spam free.</p> <p>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.</p> <p>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.</p> <p>If messages match a <i>message filter</i> and are not dropped or bounced by the filter, they are treated as clean. Messages dropped or bounced by a message filter are not counted in the totals.</p> |

**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.

## Incoming Mail Page

The **Email > Reporting > Incoming Mail** page on the Security Management appliance provides interactive reporting on the real-time information for all remote hosts connecting to your managed Security Management appliances. You can gather information about the IP addresses, domains, and network owners (organizations) sending mail to your system. You can also perform a Sender Profile search on IP addresses, domains, or organizations that have sent mail to you.

The **Incoming Mail** page It consists of two main sections: the mail trend graphs summarizing the top senders (by total threat messages and by total clean messages) and the Incoming Mail Details interactive table.

The Incoming Mail Details interactive table displays detailed information about the particular IP address, domain, or network owner (organization). You can access a Sender Profile page for any IP address, domain, or network owner by clicking the corresponding link at the top of the **Incoming Mail** page, or on other Sender Profile pages.

From the Incoming Mail pages you can:

- Perform a search on IP addresses, domains, or network owners (organizations) that have sent mail to your Security Management appliances.
- View the Sender Groups report to monitor connections according to the specific sender group and mail flow policy actions. See the [“Sender Groups Report Page” section on page 4-30](#) for more information.
- See detailed statistics on senders that have sent mail to your appliances. The statistics include the number of attempted messages broken down by security service (reputation filtering, anti-spam, anti-virus, and so forth).
- 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 examine the relationship between specific IP addresses, domains, and organizations to obtain information about a sender.
- 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.
- Obtain more information about a specific sender who has sent a high volume of spam or virus email, as determined by the anti-spam or anti-virus security services.

## Views Within the Incoming Mail Page

The **Incoming Mail** page has three different views:

- IP Addresses
- Domains



- Network Owners

These views provide a snapshot of the remote hosts connecting to the system in the context of the selected view.

Additionally, in the Incoming Mail Details section of the Incoming Mail Page, you can click on a Senders IP Address, Domain name, or Network Owner Information to retrieve specific Sender Profile Information. For more information on Sender Profile information, see the [“Sender Profile Pages” section on page 4-25](#).

**Note**

---

*Network owners* are entities that contain domains. *Domains* are entities that contain IP addresses.

---

Depending on the view you select, the Incoming Mail Details interactive table displays the top IP addresses, domains, or network owners that have sent mail to all public listeners configured on the Email Security appliances. You can monitor the flow of all mail into your appliances.

Click an IP address, domain, or network owner to access details about the sender on the Sender Profile page. The Sender Profile page is an Incoming Mail page that is specific to a particular IP address, domain, or network owner.

Click the **Sender Groups Report** link at the bottom of the Incoming Mail page to access the mail flow information by sender group.

## Categorizing Email Messages on Incoming Mail Page

Messages reported on the Incoming Mail page are categorized as follows:

**Table 4-4**      **Email Categories on Incoming Mail Page**

| Category                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Stopped by Reputation Filtering</b> | <p>All connections blocked by HAT policies multiplied by a fixed multiplier (see the <a href="#">“How Incoming Mail Messages are Counted” section on page 4-15</a>) plus all recipients blocked by recipient throttling.</p> <p>The value for Stopped by Reputation Filtering is calculated based on several factors:</p> <ul style="list-style-type: none"> <li>• Number of “throttled” messages from this sender</li> <li>• Number of rejected or TCP refused connections (may be a partial count)</li> <li>• A conservative multiplier for the number of messages per connection</li> </ul> <p>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”; that is, at least this many messages were stopped.</p> |
| <b>Invalid Recipients</b>              | All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Spam Messages Detected</b>          | The total count of messages detected by the anti-spam scanning engine as positive or suspect. Additionally, messages that are both spam and virus positive.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Virus Messages Detected</b>         | The total count and percentage of messages detected as virus positive and not also spam.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Stopped by Content Filter</b>       | The total count of messages that were stopped by a content filter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 4-4**      **Email Categories on Incoming Mail Page**

| Category                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Marketing Messages      | The total count and percentage of messages detected as unwanted marketing messages. This list item appears on the page only if marketing data are present in the system                                                                                                                                                                                                                                                                                     |
| Clean Messages Accepted | Mail that is accepted and that 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**

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.

Additionally, if messages match a *message filter* and are not dropped or bounced by the filter, they are treated as clean. Messages dropped or bounced by a message filter are not counted in the totals.

In some cases, some of the report pages contain several unique sub-reports that can be accessed from the top-level page. For example, the Incoming Mail report page on the Security Management appliance allows you to see information for individual IP Addresses, Domains and Network Owners. Each of these are sub-pages are accessed from the Incoming Mail report page.

Results for each of these sub-report pages are generated on one consolidated report when you click on the Printable PDF link at the top-right of the top-level page; in this case the Incoming Mail report page. See important information in [Understanding the Email Reporting Pages, page 4-11](#).

To view the **Incoming Mail** page, perform the following:

- Step 1**      On the Security Management appliance, choose **Email > Reporting > Incoming Mail**.

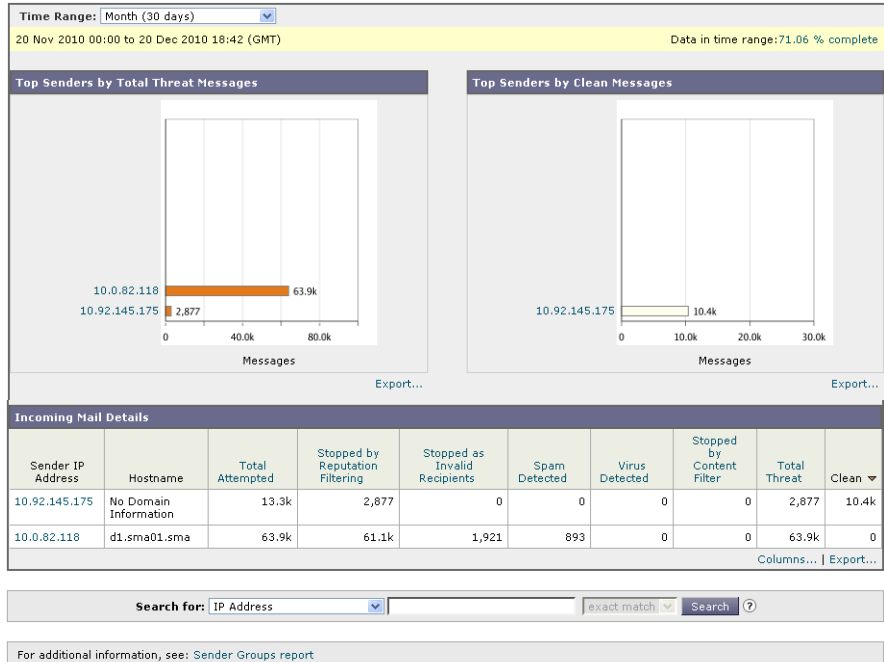
The Incoming Mail Page appears. In this example, the **IP Address** view is selected.

**Figure 4-3 Incoming Mail Page: IP Address View**

#### Incoming Mail: IP Addresses

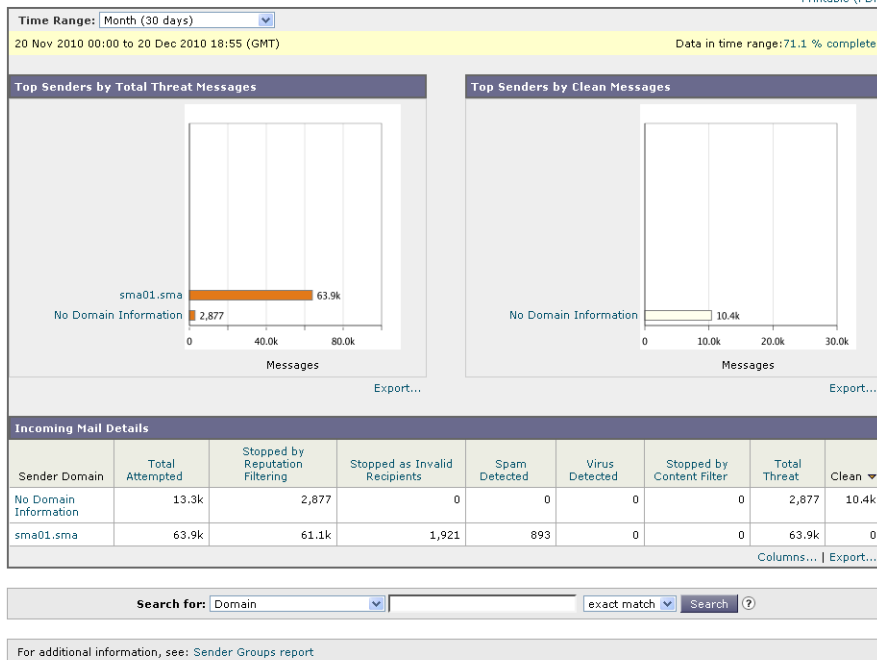
[ IP Addresses | Domains | Network Owners ]

[Printable \(PDF\)](#)



See the “[Incoming Mail Details Table](#)” section on page 4-24 for an explanation of the data included in the Incoming Mail Details interactive table.

In this example, the **Domain** view is selected.

**Figure 4-4 Incoming Mail Page: Domain View****Incoming Mail: Domains**[ IP Addresses | **Domains** | Network Owners ][Printable \(PDF\)](#)

From the **Incoming Mail** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages”](#) section on page 4-11.

**Note**

You can generate a scheduled report for the Incoming Mail report page. See the [“Scheduled Reports”](#) section on page 4-75.

**“No Domain Information” Link**

Domains that have connected to the Security Management appliances and could not be verified with a double-DNS lookup are automatically grouped into the special domain called “No Domain Information.” You can control how these types of unverified hosts are managed via Sender Verification. For more information about Sender Verification, see the *Cisco IronPort AsyncOS for Email Security Configuration Guide*.

You can use the Items Displayed menu to select the number of senders to display in the list.

## Time Ranges in the Mail Trend Graphs

You can select varying degrees of granularity to see your data in a mail graph. You can select a day, week, month, and year views of the same data. Because the data is monitored in real time, information is periodically updated and summarized in the database.

For more information on time ranges, see [“Choosing a Time Range for Interactive Reports” section on page 3-18.](#)

## Incoming Mail Details Table

The interactive Incoming Mail Details table at the bottom of the **Incoming Mail** page lists the top senders that have connected to public listeners on the Email Security appliances. The table shows domains, IP addresses, or network owners, based on the view selected. Click the column headings to sort the data.

The system acquires and verifies the validity of the remote host’s IP address by performing a *double DNS lookup*. For more information about double DNS lookups and sender verification, see the *Cisco IronPort AsyncOS for Email Security Configuration Guide*.

For senders, that is Network Owner, IP Address or Domain, listed in the first column of the Incoming Mail Details table, or on the Top Senders by Total Threat Messages, click the **Sender** or **No Domain Information** link to view more information about the sender. The results appear on a **Sender Profile** page, which includes real-time information from the Cisco IronPort SenderBase Reputation Service. From the Sender Profile page, you can view for more information about specific IP addresses or network owners. For more information, see the [“Sender Profile Pages” section on page 4-25.](#)

You can also view the Sender Groups report, by clicking **Sender Groups report** at the bottom of the Incoming Mail page. For more information about the Sender Groups report page, see the [“Sender Groups Report Page” section on page 4-30.](#)

## Sender Profile Pages

When you click a sender in the Incoming Mail Details interactive table, on the **Incoming Mail** page, the Sender Profile page appears. It shows detailed information about the particular IP address, domain, or network owner (organization). You can access a Sender Profile page for any IP address, domain, or network owner by clicking the corresponding link on the Incoming Mail page or on other Sender Profile pages.

*Network owners* are entities that contain domains. *Domains* are entities that contain IP addresses.

The Sender Profile pages displayed for IP addresses, domains, and network owners vary slightly. For each, the page contains a graph and summary table for incoming mail from the particular sender. Below the graph, a table lists the domains or IP addresses associated with the sender. (The Sender Profile page for an individual IP address does not contain a more granular listing.) The Sender Profile page also includes 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 4-5 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. 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 **More from SenderBase** to see a page with all information supplied by the SenderBase Reputation Service.

- Details about the domains and IP addresses controlled by this network owner appear on network owner profile pages. Details about the IP addresses in the domain appear on domain pages.



From a domain profile page, you can click on a specific IP address to view specific information, or view an organization profile page.

**Figure 4-6** *Current Information for Network Owner*

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

Figure 4-7 Domain Profile Page

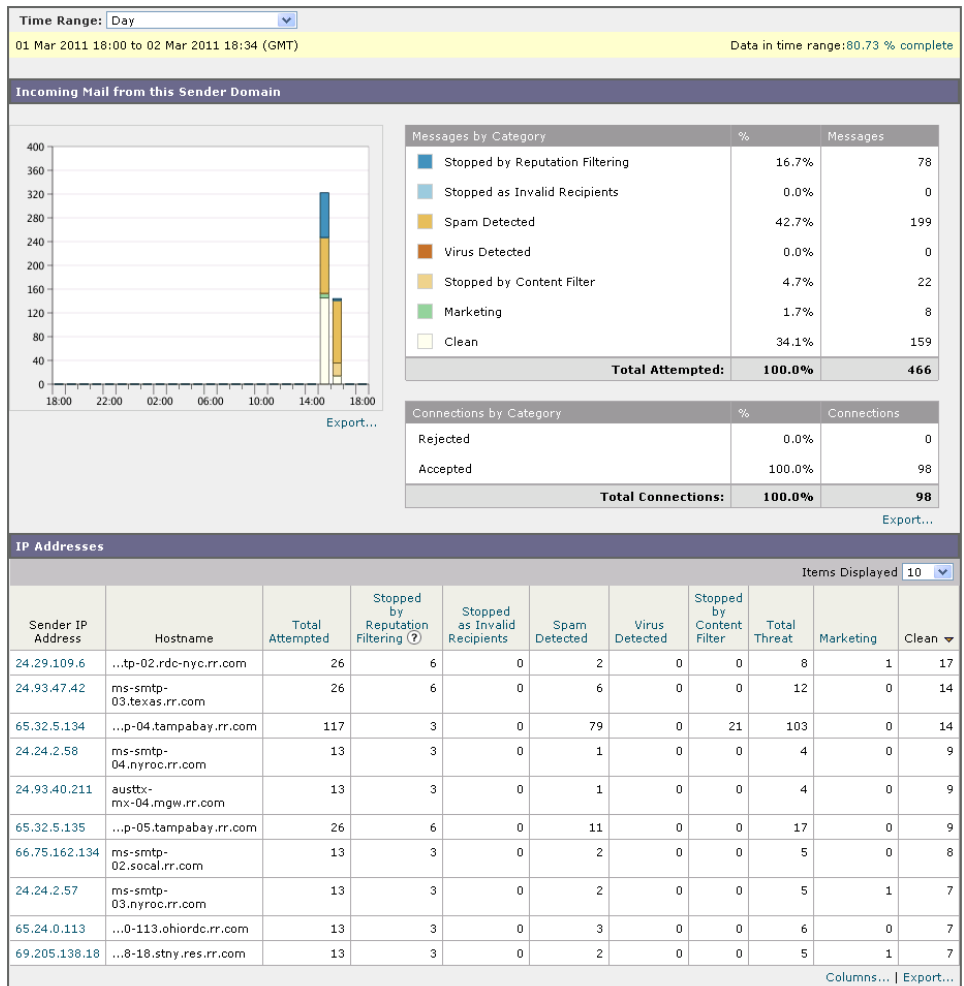


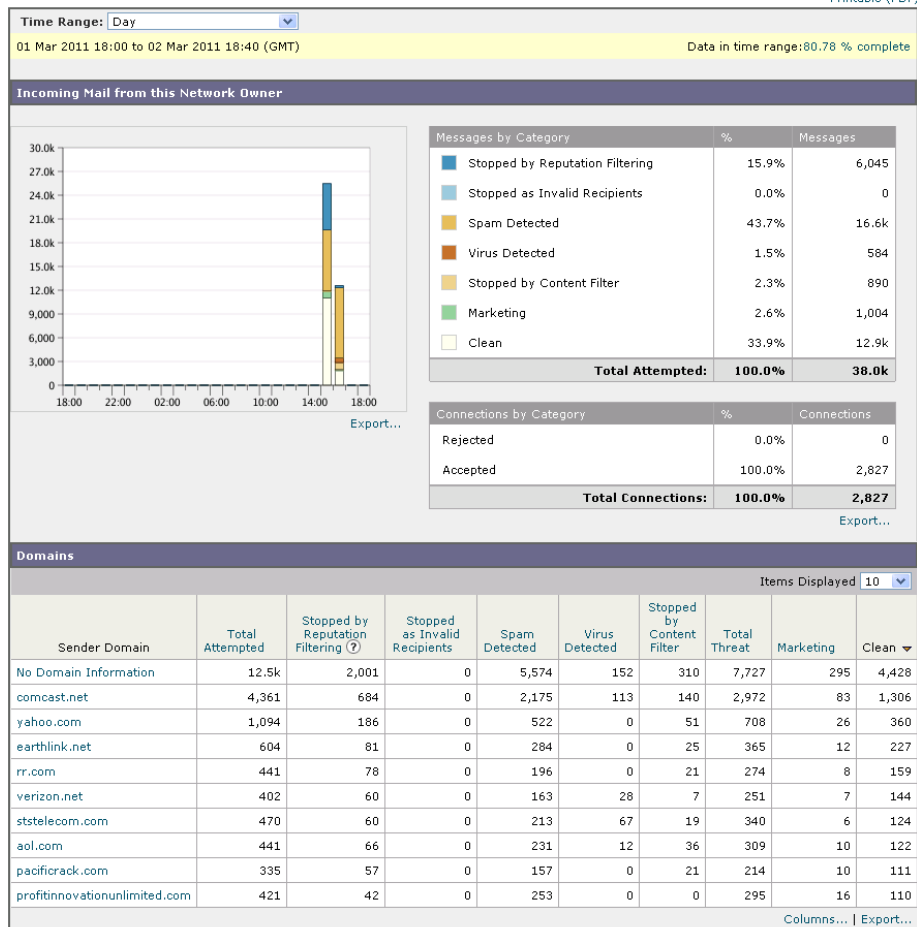
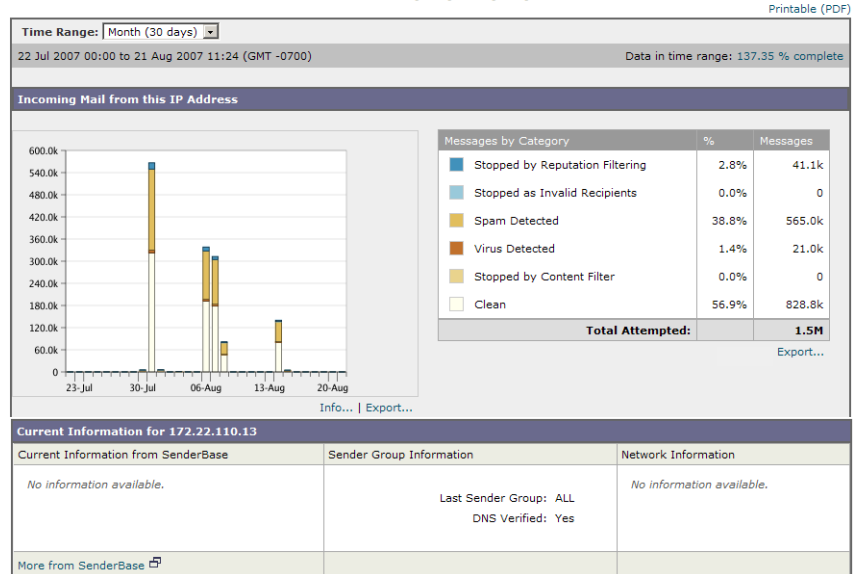
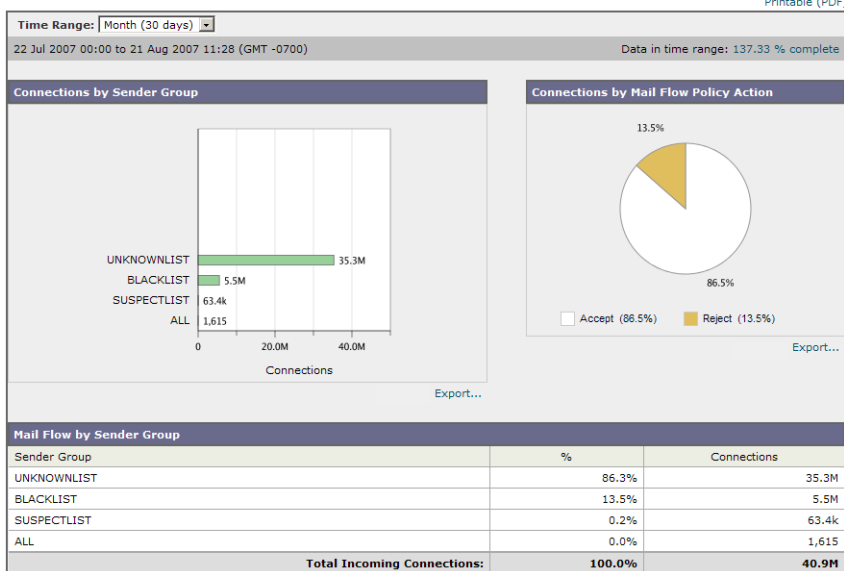
**Figure 4-8 Network Owner Profile Page****Sender Profile: Test Inc.**[Printable \(PDF\)](#)

**Figure 4-9 IP Address Profile Page****Sender Profile: 172.22.110.13 - a013.d2.prep10.prep**

## Sender Groups Report Page

The **Sender Groups report** page 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 *Cisco IronPort AsyncOS for Email Security Configuration Guide*.

**Figure 4-10 Sender Groups Report Page****Sender Groups**

From the **Sender Group report** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages” section on page 4-11](#).

**Note**

You can generate a scheduled report for the Sender Group report page. See the [“Scheduled Reports” section on page 4-75](#).

## Outgoing Destinations Page

The Outgoing Destinations page provides information about the domains that your organization sends mail to.

Use the Outgoing Destinations page to answer the following types of questions:

- Which domains are the Email Security appliances 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 servers?

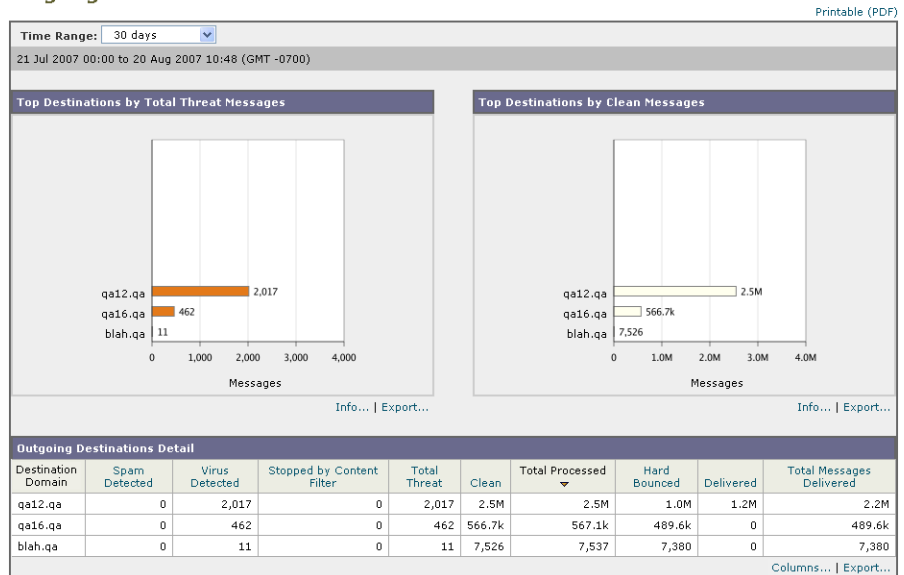
To view the Outgoing Destinations page, perform the following:

**Step 1** On the Security Management appliance, choose **Email > Reporting > Outgoing Destinations**.

The Outgoing Destinations page appears.

**Figure 4-11** *Email > Reporting > Outgoing Destinations Page*

#### Outgoing Destinations



The following list explains the various sections on the **Outgoing Destinations** page:

**Table 4-5** *Details on the Email > Reporting > Outgoing Destinations Page*

| Section                                  | Description                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>       | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| <b>Top Destination by Total Threat</b>   | The top destination domains of outgoing threat messages (spam, antivirus, etc.) sent by your organization. Total threat include threats that are spam or virus positive or that triggered a content filter.                                     |
| <b>Top Destination by Clean Messages</b> | The top destination domains of clean outgoing messages sent by your organization.                                                                                                                                                               |
| <b>Outgoing Destination Details</b>      | All details related to the destination domains of all outgoing messages sent by your organization, sorted by total recipients. Details include detected spam, viruses, clean messages etc.                                                      |

From the **Outgoing Destinations** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages”](#) section on page 4-11.



**Note**

You can generate a scheduled report for the Outgoing Destinations page. See the [“Scheduled Reports”](#) section on page 4-75.

## Outgoing Senders Page

The **Email > Outgoing Senders** page provides information about the quantity and type of mail being sent from IP addresses and domains in your network.

Use the Outgoing Senders page 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?

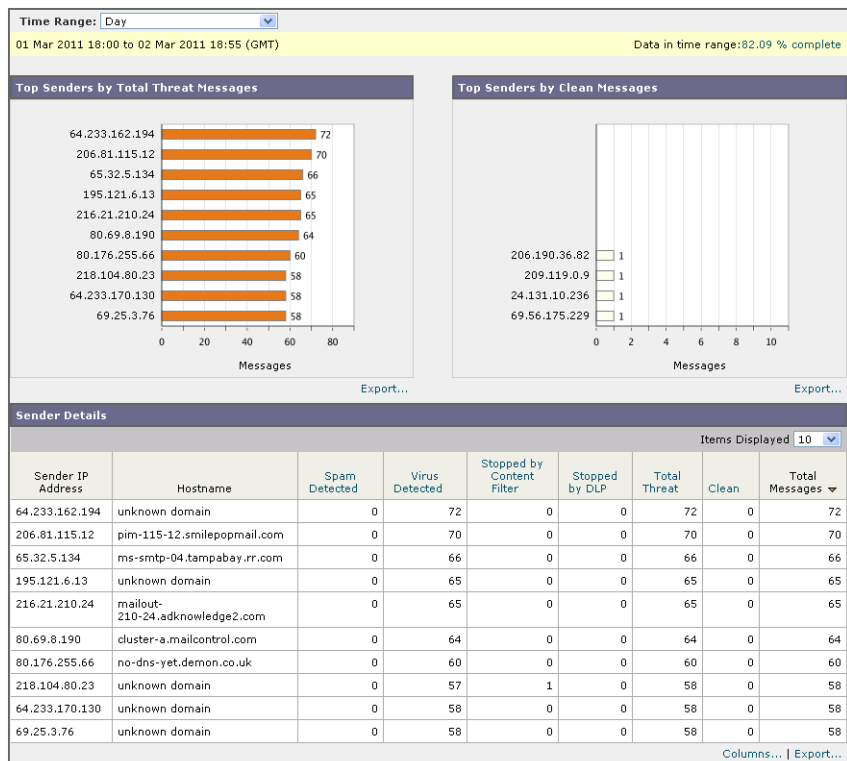
- What are the total number of recipients that are being processed where a delivery was attempted.

To view the **Outgoing Sender** page, perform the following:

**Step 1** On the Security Management appliance, choose **Email > Reporting > Outgoing Sender**.

The Outgoing Sender page appears.

**Figure 4-12** *Email > Reporting > Outgoing Senders Page (IP Addresses Displayed)*



You can see the results of the Outgoing senders with two types of views:



- **Domain:** This view allows you to see the volume of mail that is being sent by each domain
- **IP address:** This view allows you to see which IP addresses are sending the most virus messages or triggering content filters.

The following list explains the various sections on the **Outgoing Senders** page for both views:

**Table 4-6**      *Details on the Email > Reporting > Outgoing Sender Page*

| Section                                     | Description                                                                                                                                                                                                                                     |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>          | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| <b>Top Senders by Total Threat Messages</b> | The top senders (by IP address or domain) of outgoing threat messages (spam, antivirus, etc.) in your organization.                                                                                                                             |
| <b>Top Sender by Clean Messages</b>         | The top senders (by IP address or domain) of clean outgoing messages sent in your organization.                                                                                                                                                 |
| <b>Sender Details</b>                       | All details on the senders (by IP address or domain) of all outgoing messages sent by your organization. Details include detected spam, viruses, clean messages, etc.                                                                           |



**Note**

This page does not display information about message delivery. To track delivery information, such as the number of messages from a particular domain that were bounced, log in to the appropriate Email Security appliance and choose **Monitor > Delivery Status**.

From the **Outgoing Senders** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages”](#) section on page 4-11.



**Note**

You can generate a scheduled report for the **Outgoing Senders** page. See the [“Scheduled Reports”](#) section on page 4-75.

## 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 can have multiple email addresses. The email addresses are not combined in the report.

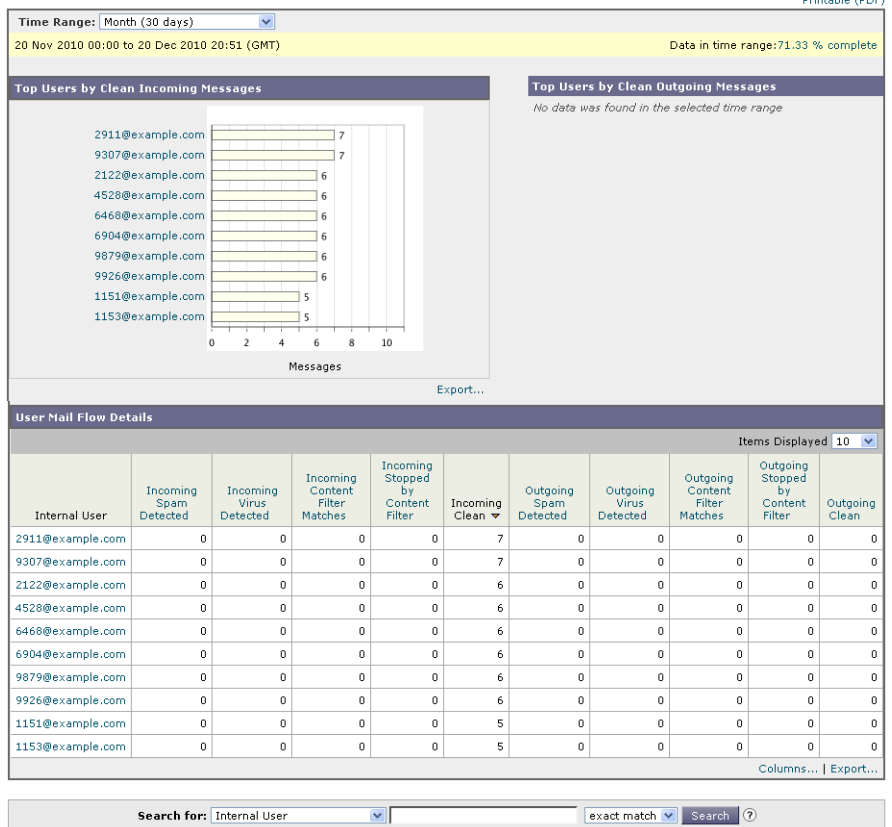
Use the Internal Users interactive report page to answer these types of questions:

- Who sends the most external email?
- Who receives the most clean email?
- Who receives the most spam?
- Who is triggering particular content filters?
- Are content filters stopping email from a particular user?

To view the **Internal Users** page, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Email > Reporting > Internal Users**.

The Internal Users page appears.

**Figure 4-13** *Email > Reporting> Internal Users Page***Internal Users**

The following list explains the various sections on the **Internal Users** page for both views:

**Table 4-7**      *Details on the Email > Reporting > Internal Users Page*

| Section                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>          | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                                                                                                       |
| <b>Top Users by Clean Incoming Messages</b> | The top users by (by IP address or domain) of clean incoming messages sent in your organization.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Top Users by Clean Outgoing Messages</b> | The top users (by IP address or domain) of clean outgoing messages sent in your organization.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>User Mail Flow Details</b>               | <p>The User Mail Flow Details interactive section 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 the column headers.</p> <p>Click an internal user in the Internal User column to view the Internal User Detail page for that user. For more information on the Internal Users Details page, see the <a href="#">“Internal User Details Page”</a> section on page 4-38.</p> |

From the **Internal Users** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages”](#) section on page 4-11.



**Note**

You can generate a scheduled report for the Internal Users page. See the [“Scheduled Reports”](#) section on page 4-75.

# Internal User Details Page

The Internal User detail page shows detailed information about a 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 matches are also shown.

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.

Click a content filter name to view detailed information for that filter on the corresponding content filter information page (see [Content Filters Page, page 4-43](#)). You can use this method to view a list of all users who sent or received mail that matched the particular content filter.



#### Note

Some outbound mail (such as bounces) has a null sender. They are counted as outbound “unknown.”

## Searching for a Specific Internal User

With the search form at the bottom of the Internal Users page and the Internal User detail page, you can search for a specific internal user (email address). Select whether to exactly match the search text or look for items starting with the entered text (for example, starts with “ex” will match “example@example.com”).

**Figure 4-14 Internal User Search Results**

#### Search Results

[Printable \(PDF\)](#)

| Search for: Internal User user1@example.com exact match Search ?                                            |                        |                         |                                 |                                    |                |                        |                         |                                 |                                    |                |
|-------------------------------------------------------------------------------------------------------------|------------------------|-------------------------|---------------------------------|------------------------------------|----------------|------------------------|-------------------------|---------------------------------|------------------------------------|----------------|
| Time Range: Day<br>26 Apr 2011 15:00 to 27 Apr 2011 15:41 (GMT -07:00) Data in time range: 99.36 % complete |                        |                         |                                 |                                    |                |                        |                         |                                 |                                    |                |
| <b>Search Results for Internal Users</b><br>1 item found matching "user1@example.com"                       |                        |                         |                                 |                                    |                |                        |                         |                                 |                                    |                |
| Internal User                                                                                               | Incoming Spam Detected | Incoming Virus Detected | Incoming Content Filter Matches | Incoming Stopped by Content Filter | Incoming Clean | Outgoing Spam Detected | Outgoing Virus Detected | Outgoing Content Filter Matches | Outgoing Stopped by Content Filter | Outgoing Clean |
| user1@example.com                                                                                           | 14                     | 0                       | 13                              | 0                                  | 16.3k          | 0                      | 0                       | 0                               | 0                                  | 0              |
| Columns...   Export...                                                                                      |                        |                         |                                 |                                    |                |                        |                         |                                 |                                    |                |

## DLP Incident Summary Page

The DLP Incident Summary 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 Incident Summary report, you can answer these kinds of questions:

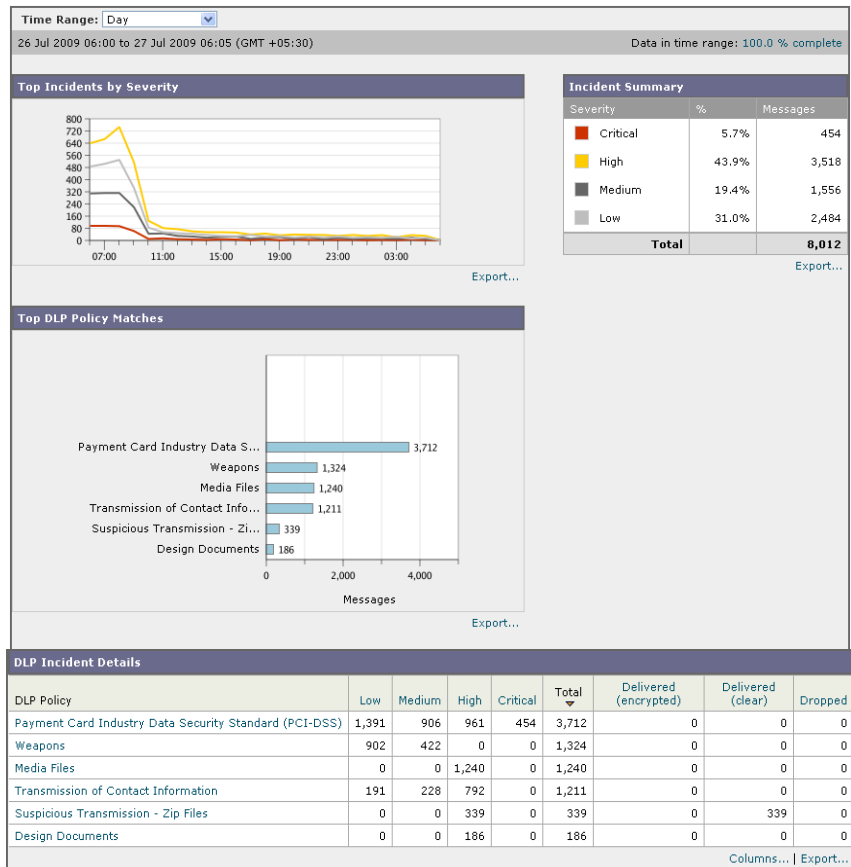
- What type of sensitive data is being sent by your users?
- How severe are these DLP incidents?
- How many of these messages are being delivered?
- How many of these messages are being dropped?
- Who is sending these messages?

To view the DLP Summary page, perform the following:

---

**Step 1** On the Security Management appliance, choose **Email > Reporting > DLP Summary**.

The DLP Summary page appears.

**Figure 4-15** *Email > Reporting > DLP Incidents Summary Page*

The DLP Incident Summary page contains two main sections:

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

The following list explains the various sections on the **DLP Incident Summary** page:

**Table 4-8**      *Details on the Email > Reporting > DLP Incident Summary Page*

| Section                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b> | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                          |
| <b>Top Incidents by Severity</b>   | The top DLP incidents listed by severity.                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Incident Summary</b>            | The DLP policies currently enabled for each email appliance’s outgoing mail policies are listed in the DLP Incident Details interactive table at the bottom of the <b>DLP Incident Summary</b> page. Click the name of a DLP policy to view more detailed information.                                                                                                                                                                   |
| <b>Top DLP Policy Matches</b>      | The top DLP Policies that have been matched.                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>DLP Incident Details</b>        | <p>The DLP Incident Details table shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped.</p> <p>Click the name of a DLP policy to view more detailed information. For more information on the DLP Incidents Details page, see the <a href="#">“DLP Incidents Details Table”</a> section on page 4-42.</p> |

Click 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 Table

The DLP Incident Details table is an interactive table that shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped. Click the column headings to sort the data. To find out more information about



any of the DLP Policies listed in this interactive table, click on the name of the DLP Policy and the DLP Policy Page appears. For more information, see [“DLP Policy Detail Page” section on page 4-43](#).

## DLP Policy Detail Page

If you click on a name of a DLP policy in the DLP Incident 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 by Severity.

The page also includes an Incidents by Sender table at the bottom of the page that lists each internal user who has sent a message that violated the DLP policy. The table 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 table to find out which users may be sending your organization’s sensitive data to people outside your network.

Clicking the sender name opens up the Internal Users page. See the [“Internal Users Page” section on page 4-36](#) for more information.

## Content Filters Page

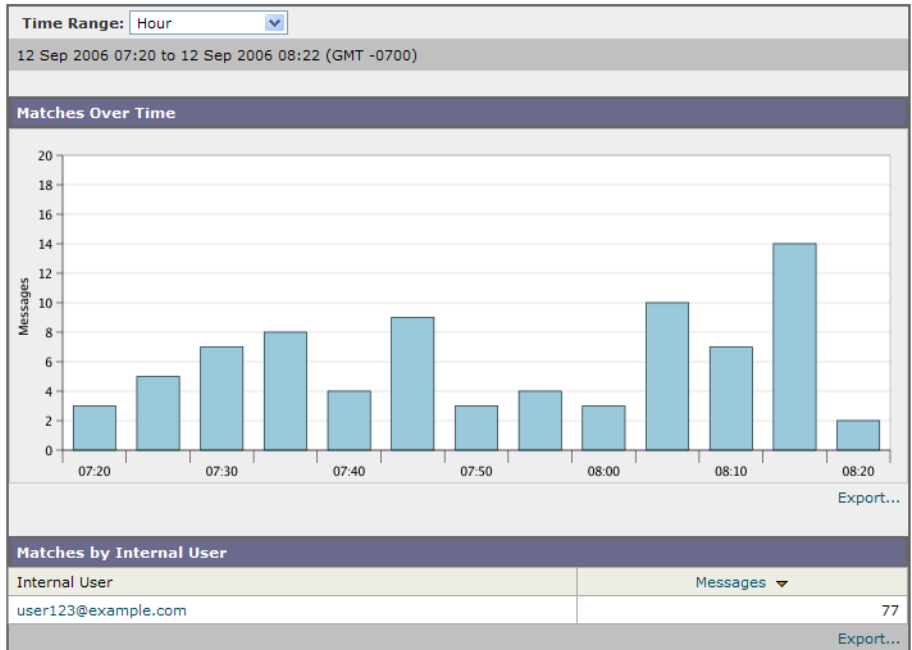
The Content Filters page shows information about the top incoming and outgoing content filter matches (which content filter had the most matching messages). The page displays the data as both bar charts and listings. Using the Content Filters page, you can review your corporate policies on a per-content-filter or per-user basis and answer the following types of questions:

- Which content filter is triggered the most by incoming or outgoing mail?
- Who are the top users sending or receiving mail that triggers a particular content filter?

To view the Content Filter page, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Email > Reporting > Content Filters**.

The **Content Filters** page appears.

**Figure 4-16** *Email > Reporting > Content Filters Page***Outgoing Content Filter: free\_stuff**[Printable \(PDF\)](#)

To view more information about a specific filter, click the name of the filter. The Content Filter Details page appears. For more information on Content Filter details page, see the [“Content Filter Details Page”](#) section on page 4-45.

From the **Content Filters** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages”](#) section on page 4-11.

**Note**

You can generate a scheduled report for the Content Filter page. See the [“Scheduled Reports”](#) section on page 4-75.

## Content Filter Details Page

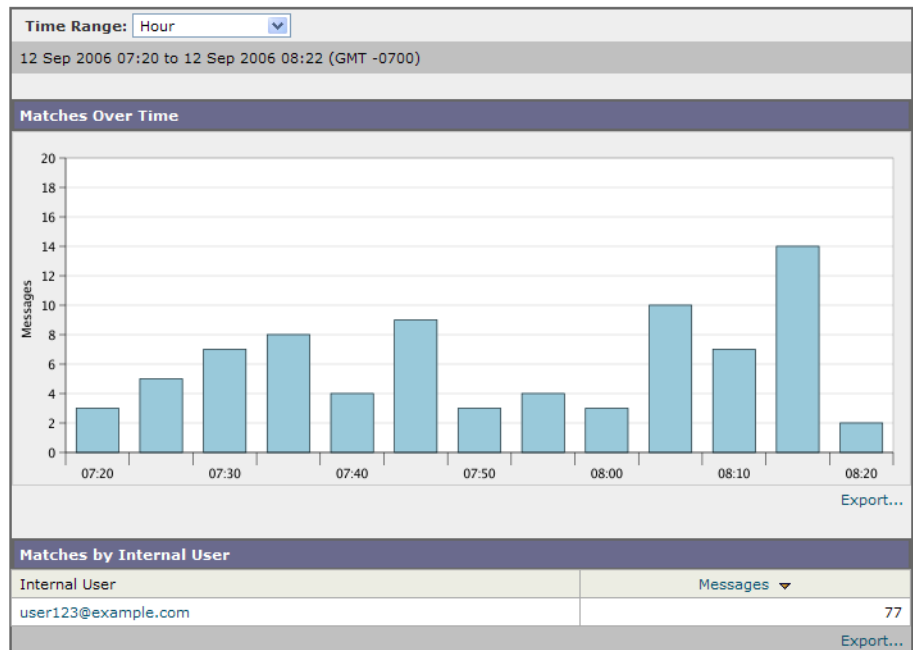
The Content Filter Detail page displays matches for the filter over time, as well as matches by internal user.

In the Matches by Internal User section, click the name of a user to view the detail page for the internal user (email address). For more information, see [Internal User Details Page, page 4-38](#).

**Figure 4-17**      **Content Filters Details Page**

### Outgoing Content Filter: free\_stuff

[Printable \(PDF\)](#)



## Virus Types Page

The Virus Types page provides an overview of the viruses that are sent to and from your network. The Virus Types page displays the viruses that have been detected by the virus scanning engines running on the Email Security appliances and are displayed on the Security Management appliance. Use this report to take action

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



#### Note

Outbreak Filters can quarantine these types of virus-infected messages with no user intervention.

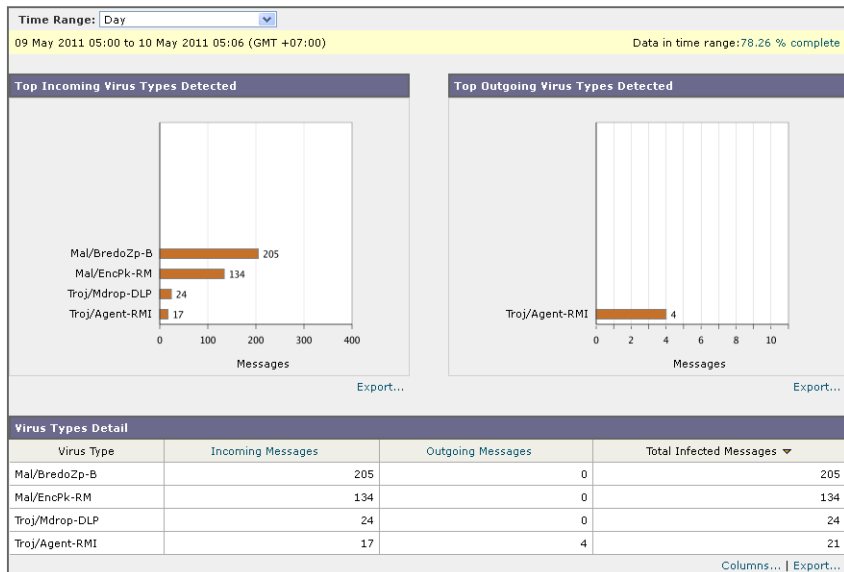
To view the Virus Types page, perform the following:

**Step 1** On the Security Management appliance, choose **Email > Reporting > Virus Types**.

The **Virus Types** page appears.

**Figure 4-18** *Email > Reporting > Virus Types Page*

#### Virus Types



If you run multiple virus scanning engines, the Virus Types page includes results from all enabled virus scanning engines. The name of the virus that appears on the page is 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 following list explains the various sections on the **Virus Types** page:

**Table 4-9**      **Details on the Email > Reporting > Virus Types Page**

| Section                                  | Description                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>       | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| <b>Top Incoming Virus Types Detected</b> | This section displays a chart view of the viruses that have been sent to your network.                                                                                                                                                          |
| <b>Top Outgoing Virus Types Detected</b> | This section displays a chart view of the viruses that have been sent from your network.                                                                                                                                                        |
| <b>Virus Types Detail</b>                | An interactive table that shows the details of each virus type.                                                                                                                                                                                 |



**Note**

To see which hosts sent virus-infected messages to your network, 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, view the Outgoing Senders page and sort by virus positive messages.

From the **Virus Types** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Understanding the Email Reporting Pages”](#) section on page 4-11.



**Note**

You can generate a scheduled report for the **Virus Types** page. See the [“Scheduled Reports”](#) section on page 4-75.

## TLS Connections Page

The TLS Connections page 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 uses TLS?
- Which partners do I have successful TLS connections with?
- Which partners do I have unsuccessful TLS connections with?
- Which partners have issue with their TLS certificates?
- What percentage of overall mail with a partner uses TLS?

To view the TLS Connections page, perform the following:

---

**Step 1** On the Security Management appliance, choose **Email > Reporting > TLS Connections**.

The **TLS Connections Report** page appears.

The TLS Connections Report page is divided into two major sections:

- [TLS Connections Report Page: Incoming Connections](#)
- [TLS Connections Report Page: Outgoing Connections](#)

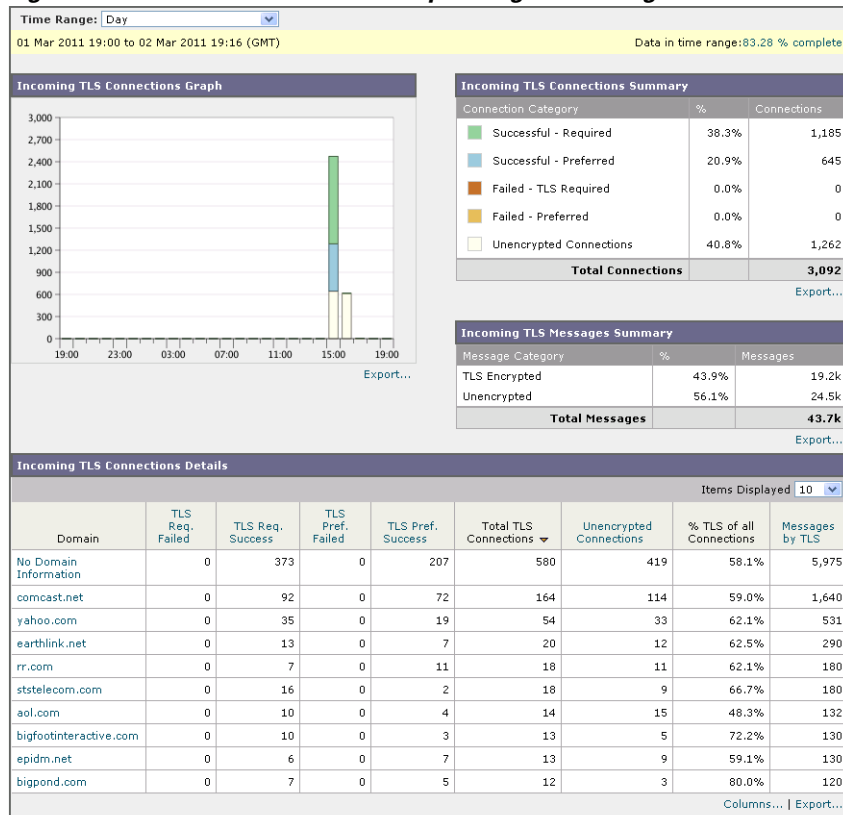
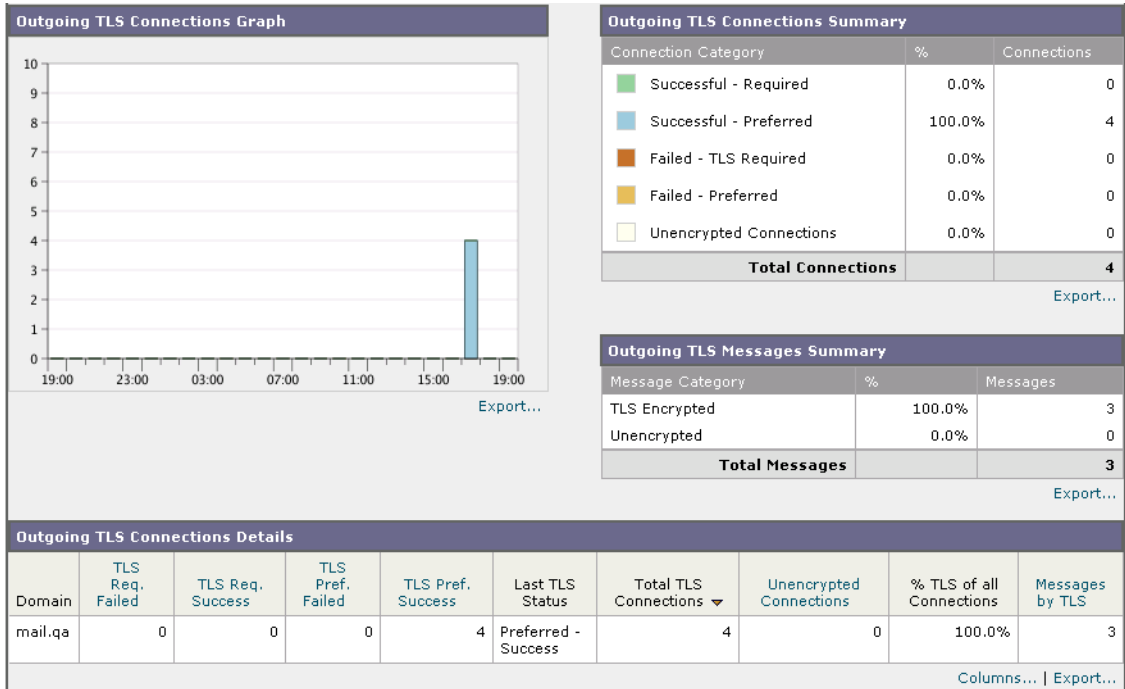
**Figure 4-19 TLS Connections Report Page: Incoming Connections**

**Figure 4-20 TLS Connections Report Page: Outgoing Connections**

The following list explains the various sections on the **TLS Connections** page:

**Table 4-10 Details on the Email > Reporting > TLS Connections Page**

| Section                                 | Description                                                                                                                                                                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>      | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| <b>Incoming TLS Connections Graph</b>   | The graph displays a view of incoming TLS encrypted and unencrypted connections over the last hour, day, or week depending on the time frame that you have selected.                                                                            |
| <b>Incoming TLS Connections Summary</b> | This table displays the total volume of incoming messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed incoming TLS encrypted messages.                                                           |



**Table 4-10**      *Details on the Email > Reporting > TLS Connections Page*

| Section                                 | Description                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Incoming TLS Message Summary</b>     | This table displays a summary of the total volume of incoming messages.                                                                                                                                                                                                                                                                         |
| <b>Incoming TLS Connections Details</b> | The table displays details for domains sending or receiving encrypted messages. For each domain, you can view the total number of connections, messages sent, and the number of TLS connections that were successful or failed. You can also view the percentage of successful and failed connections for each domain.                          |
| <b>Outgoing TLS Connections Graph</b>   | The graph displays a view of outgoing TLS encrypted and unencrypted connections over the last hour, day, or week depending on the time frame that you have selected.                                                                                                                                                                            |
| <b>Outgoing TLS Connections Summary</b> | This table displays the total volume of outgoing messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed outgoing TLS encrypted messages.                                                                                                                                                           |
| <b>Outgoing TLS Message Summary</b>     | This table shows the total volume of outgoing messages                                                                                                                                                                                                                                                                                          |
| <b>Outgoing TLS Connections Details</b> | The table displays details for domains sending or receiving encrypted messages. For each domain, you can view the total number of connections, messages sent, and the number of TLS connections that were successful or failed, and the last TLS status. You can also view the percentage of successful and failed connections for each domain. |

## Outbreak Filters Page

The **Outbreak Filters** page shows 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.

Use the Outbreak Filters page to answer the following types of questions:

- How many messages are quarantined and by which Outbreak Filters rule?
- How much lead time has the Outbreak Filters feature been providing for virus outbreaks?

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

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.

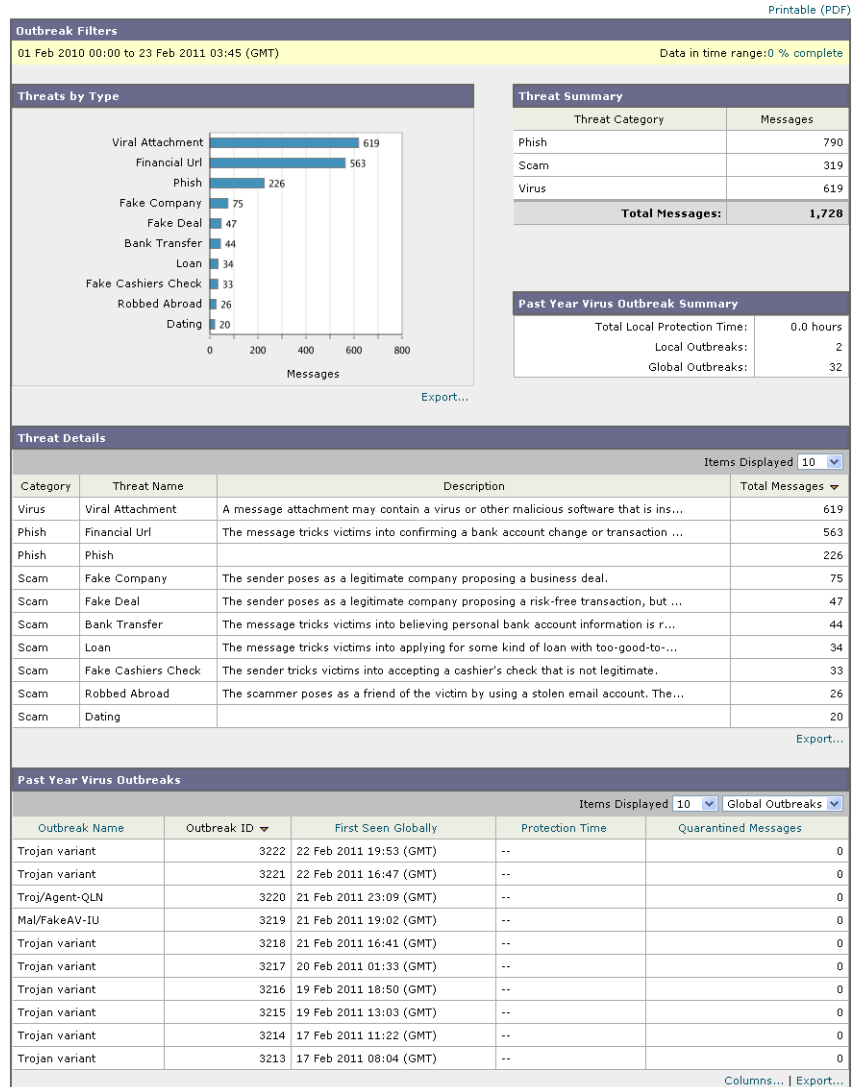
The Threat Details listing displays information about specific outbreaks, including the threat category (virus, scam, or phishing), threat name, a description of the threat, and the number of messages identified. For virus outbreaks, the Past Year Virus Outbreaks include the Outbreak name and ID, time 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.

To view the **Outbreak Filters** page, choose **Email > Reporting > Outbreak Filters**. [Figure 4-21](#) shows the Outbreak Filters page.

**Figure 4-21 Outbreaks Page****Outbreak Filters**

**Note**

The Security Management appliance must be able to communicate with `downloads.cisco.com` to correctly populate the tables on the Outbreak Filters page.

## System Capacity Page

The System Capacity page provides a detailed representation of the system load, including messages 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 Email Security appliances are exceeding recommended capacity; this enables you to determine when configuration optimization or additional appliances are needed.
- Identify historical trends in system behavior that point to upcoming capacity issues.
- For troubleshooting, identify which parts of the system are using the most resources.

Monitor your Email Security appliances to ensure that the capacity is appropriate to your message volumes. Over time, volume inevitably rises and appropriate monitoring ensures that additional capacity or configuration changes can be applied proactively. The most effective way to monitor system capacity is to track the overall volume, the messages in the work queue, and the incidents of Resource Conservation Mode.

- **Volume:** It is important to understand 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 4-57](#) and [System Capacity – Outgoing Mail, page 4-60](#).
- **Work Queue:** The work queue is designed to work as a “shock absorber”—absorbing and filtering spam attacks and processing unusual increases in non-spam messages. However, the work queue can also indicate a system under stress. Prolonged and frequent work queue backups may indicate a

capacity problem. You can use the System Capacity – Workqueue page to track the activity in your work queue. For more information, see [System Capacity – Workqueue, page 4-56](#).

- **Resource Conservation Mode:** When a Cisco IronPort appliance becomes overloaded, it enters Resource Conservation Mode (RCM) and sends 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. RCM is not tracked by the System Capacity page.

## How to Interpret the Data You See on System Capacity Page

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

- **Day Report—** The Day report queries the hour table and displays the exact number of queries that have been received by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table. This is an exact number.
- **Month Report—** The Month report queries the day tables for the 30 or 31 days (dependent on the number of days in the month), giving you an exact report on the number of queries over 30 or 31 days. Again, this is an exact number.

The ‘Maximum’ value indicator on the System Capacity page is the highest value seen for the specified period. The ‘Average’ value is the average of all values for the specified period. The period of aggregation depends on the interval selected for that report. For example, you can choose to see the Average and Maximum values for each day if the chart is for a month period.

You can click the View Details link for a specific graph to view data for individual Email Security appliances and overall data for the appliances connected to the Security Management appliance.

## System Capacity – Workqueue

The System Capacity – Workqueue page shows the volume of messages in work queues over a specified time period. It also shows the maximum messages in work queues over the same time period. You can view data for a day, week, month, or year. Occasional spikes in the Workqueue graphs are normal and expected. If the

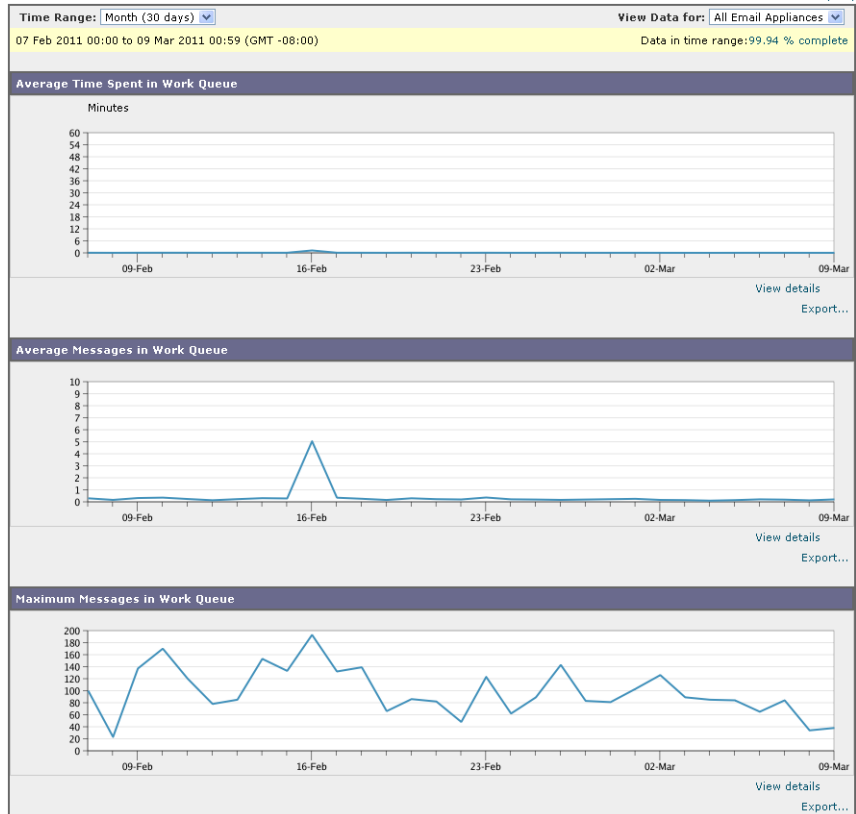
spikes occur with increasing frequency and are maintained over a long period of time, this may indicate a capacity issue. When reviewing the work queue page, you may want to measure the frequency of work queue backups, and take note of work queue backups that exceed 10,000 messages.

**Figure 4-22 System Capacity – Workqueue**

### System Capacity

[ **Workqueue** | Incoming Mail | Outgoing Mail | System Load | All ]

[Printable \(PDF\)](#)



## System Capacity – Incoming Mail

The System Capacity – Incoming Mail page shows incoming connections, the total number of incoming messages, the average message size, and the total incoming message size. You can view the results for a day, week, month, or year.

It is important to understand the trends of normal message volume and spikes in your environment. You can use the System Capacity – Incoming Mail page to 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 email messages that are sent from specific domains to your network.

**Note**

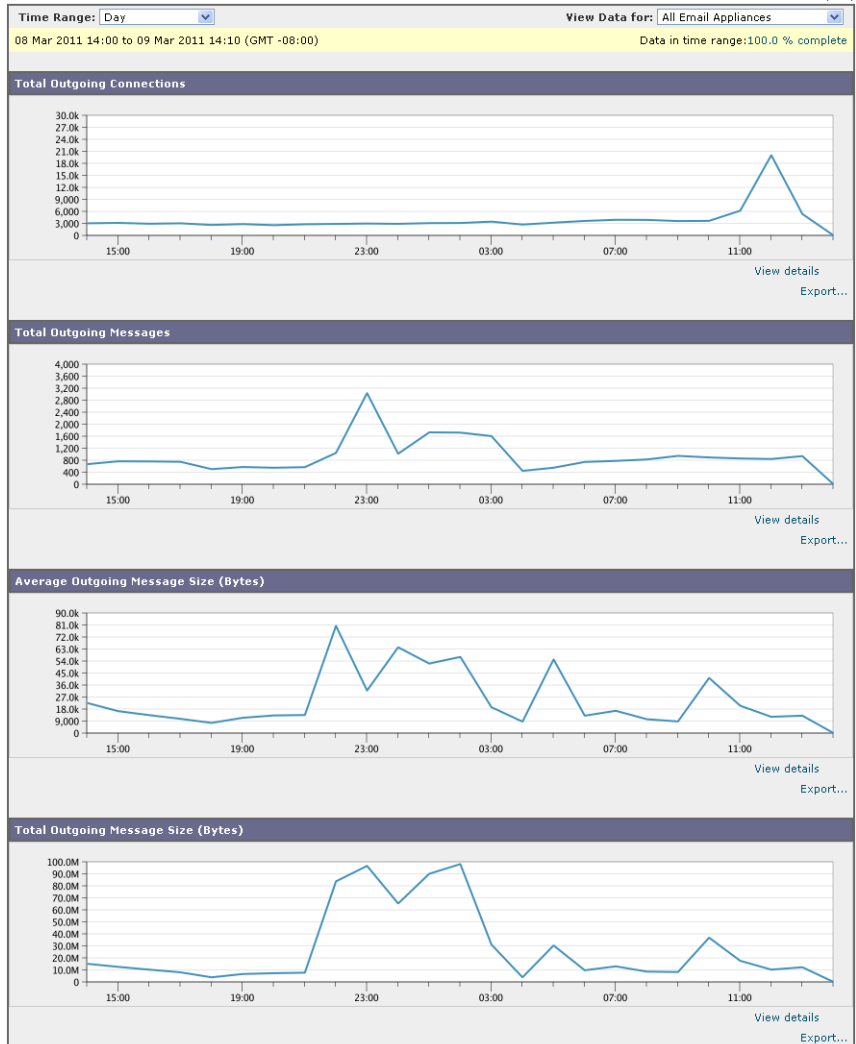
An increased number of incoming connections may not necessarily affect system load.



**Figure 4-23 System Capacity – Incoming Mail****System Capacity**[ [Workqueue](#) | [Incoming Mail](#) | [Outgoing Mail](#) | [System Load](#) | [All](#) ][Printable \(PDF\)](#)

## System Capacity – Outgoing Mail

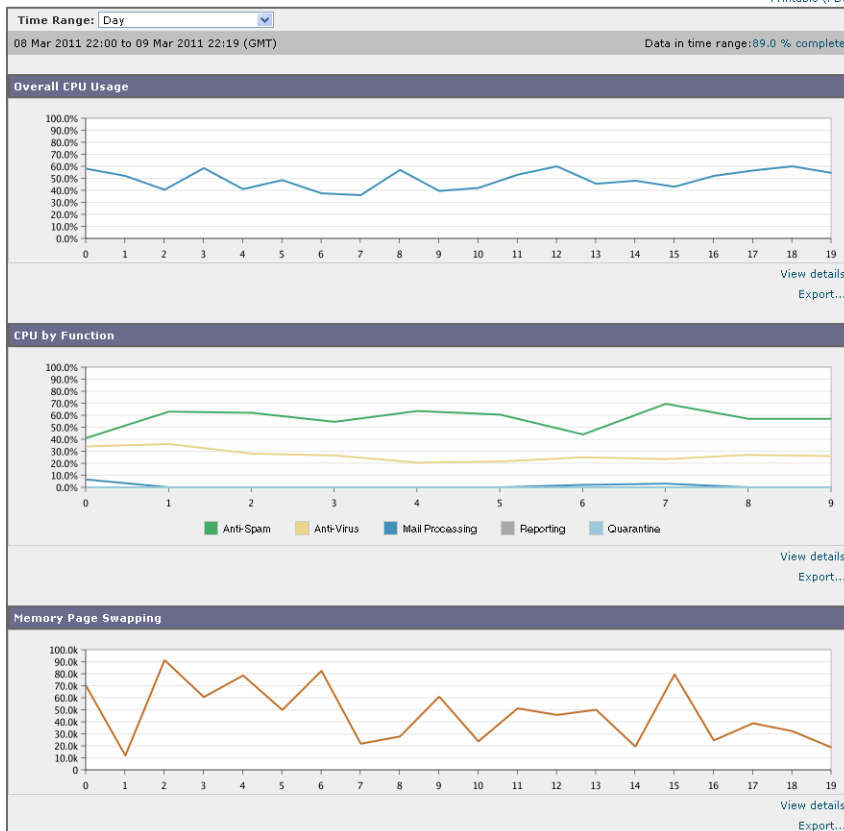
The System Capacity – Outgoing Mail page shows outgoing connections, the total number of outgoing messages, the average message size, and the total outgoing message size. You can view the results for a day, week, month, or year. It is important to understand the trends of normal message volume and spikes in your environment. You can use the System Capacity – Outgoing Mail page to 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 email messages that are sent from specific domains or IP addresses.

**Figure 4-24 System Capacity – Outgoing Mail****System Capacity**[ Workqueue | Incoming Mail | **Outgoing Mail** | System Load | All ][Printable \(PDF\)](#)

## System Capacity – System Load

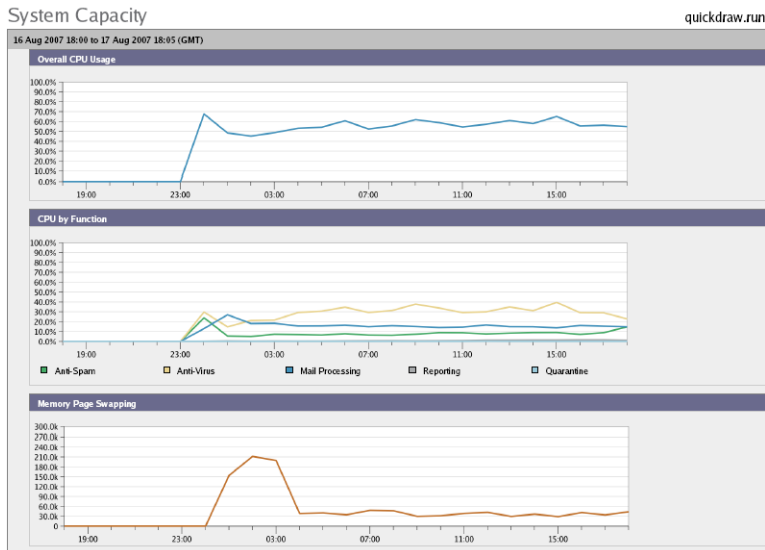
The system load report shows the overall CPU usage on the Email Security appliances. AsyncOS is optimized to use idle CPU resources to improve message throughput. High CPU usage may not indicate a system capacity problem. If the high CPU usage is coupled with consistent, high-volume memory page swapping, 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 an 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 4-25 System Capacity – System Load****System Capacity**[ Workqueue | Incoming Mail | Outgoing Mail | **System Load** | All][Printable \(PDF\)](#)

## 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 appliances). For example, [Figure 4-26](#) 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 4-26 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 see that 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 a PDF file to preserve a snapshot of system performance for later reference (or to share with support staff).

## Data Availability Page

The **Email > Reporting > Data Availability** page allows you to view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.

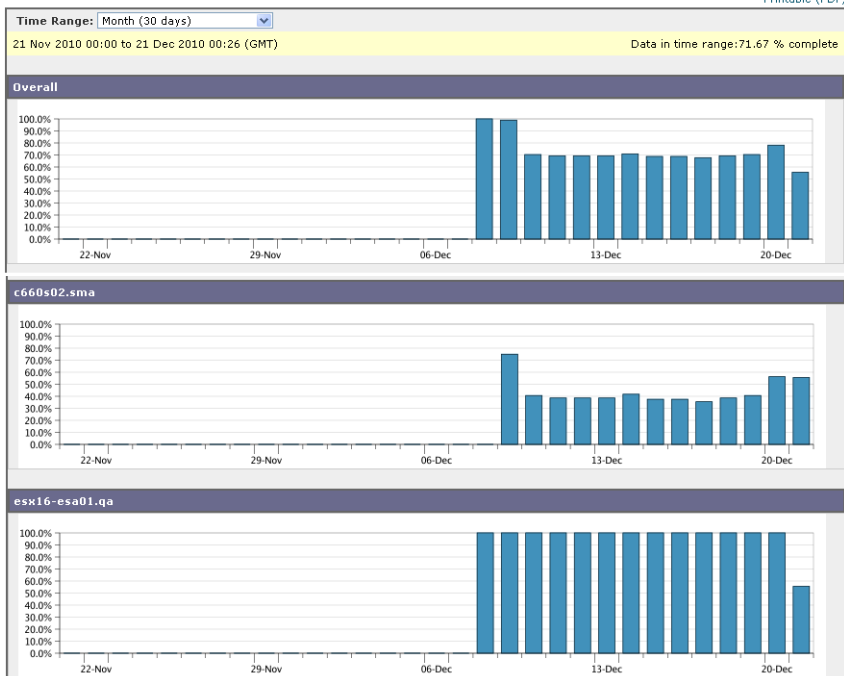
To view the **Data Availability** page, perform the following:

**Step 1** On the Security Management appliance page, choose **Email > Reporting > Data Availability**.

The **Reporting Data Availability** page appears.

**Figure 4-27 Email Reporting Data Availability Page**

#### Reporting Data Availability



All data resource utilization and email traffic trouble spots are shown from this page, including the data availability for the overall appliances that are managed by the Security Management appliance.

From this report page you can also view the data availability for a specific appliance and time range.

# About Scheduled and On-Demand Reports

## Types of Reports Available

In addition to the reports available via the interactive report pages, the following types of reports are available as scheduled and on-demand reports:

- **Content Filters**—This report includes up to 40 content filters. For additional information on what is included on this page, see the [“Content Filters Page” section on page 4-43](#).
- **DLP Incident Summary**—For information on what is included on this page, see the [“DLP Incident Summary Page” section on page 4-40](#).
- **Delivery Status**—The report page displays information about delivery problems to a specific recipient domain or Virtual Gateway address, 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. For more information on what the Delivery Status page does on the Email Security appliance, see the *Cisco IronPort AsyncOS for Email Security Daily Management Guide*.
- **Domain-Based Executive Summary**—This report is based on the [Email Reporting Overview Page](#), and is limited to a group of specified domains. For information on what is included, see the [“Domain-Based Executive Summary Report” section on page 4-68](#).
- **Executive Summary**—This report is based on the information from the [Email Reporting Overview Page](#). For information on what is included, see the [“Domain-Based Executive Summary Report” section on page 4-68](#).
- **Incoming Mail Summary** — For information on what is included on this page, see the [“Incoming Mail Page” section on page 4-17](#).
- **Internal Users Summary**—For information on what is included on this page, see the [“Internal Users Page” section on page 4-36](#).
- **Outbreak Filters**—For information on what is included on this page, see the [“Outbreak Filters Page” section on page 4-51](#).
- **Outgoing Destinations**—For information on what is included on this page, see the [“Outgoing Destinations Page” section on page 4-31](#).



- **Outgoing Mail Summary**—For information on what is included on this page, see the [“Outgoing Senders Page” section on page 4-33](#).
- **Outgoing Senders: Domains** —For information on what is included on this page, see the [“Outgoing Senders Page” section on page 4-33](#).
- **Sender Groups** —For information on what is included on this page, see the [“Sender Groups Report Page” section on page 4-30](#).
- **System Capacity**—For information on what is included on this page, see the [“System Capacity Page” section on page 4-55](#).
- **TLS Connections**—For information on what is included on this page, see the [“TLS Connections Page” section on page 4-48](#).
- **Virus Types**—For information on what is included on this page, see the [“Virus Types Page” section on page 4-45](#).

### Time ranges

Depending on the report, these reports can be configured to include data for the previous day, previous seven days, previous month, previous calendar day (up to 250), or previous calendar month (up to 12). Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months).

Regardless of when you run a report, the data is returned from the previous time interval (hour, day, week, or month). For example, if you schedule a daily report to run at 1AM, the report will contain data from the previous day, midnight to midnight (00:00 to 23:59).

### Languages and Locales



#### Note

You can schedule a PDF or CSV report with a specific locale for that individual report. The language drop-down menu on the Scheduled Reports page allows you to view or schedule a PDF report in the users current selected locale and language. See important information at [Printing and Exporting Report Data, page 3-20](#).

### Storage of Archived Reports

For information on how long reports are stored for, and when archived reports are deleted from the system, see [Archived Reports, page 4-78](#).

## Additional Report Types

Two special reports that can be generated in the **Email > Reporting** section on the Security Management appliance are:

- [Domain-Based Executive Summary Report](#)
- [Executive Summary Reports](#)

### Domain-Based Executive Summary Report

The Domain-Based Executive Summary report provides a synopsis of the incoming and outgoing message activity for one or more domains in your network. It is similar to the Executive Summary report, but it limits the report data to the messages sent to and from the domains that you specify. If multiple domains are specified, the appliance aggregates the data for all those domains into a single report. Unlike other scheduled reports, Domain-Based Executive Summary reports are not archived.

Because messages blocked by reputation filtering do not enter the work queue, AsyncOS does not process these messages to determine the domain destination. An algorithm estimates the number of rejected messages per domain. To determine the exact number of blocked messages per domain, you can delay HAT rejections on the Cisco IronPort Security Management appliance until the messages reach the recipient level (RCPT TO). This allows AsyncOS to collect recipient data from the incoming messages. You can delay rejections using **listenerconfig -> setup** command on the Cisco IronPort Email Security appliance. However, this option can impact system performance. For more information about delayed HAT rejections, see the documentation for Cisco IronPort AsyncOS for Email Security.



#### Note

To see Stopped by Reputation Filtering results in your Domain-Based Executive Summary report on the Security Management appliance, you must have **hat\_reject\_info** enabled on both the Email Security appliance and the Security Management appliance.

To enable the **hat\_reject\_info** on the Security Management appliance, run the **reportingconfig > domain > hat\_reject\_info** command.

To generate reports for a subdomain, you must add its parent domain as a second-level domain in the reporting system of the Email Security appliance and the Security Management appliance. For example, if you add example.com as a second-level domain, its subdomains, such as subdomain.example.com, are available for reporting. To add second-level domains, use **reportingconfig -> mailsetup -> tld** in the Email Security appliance CLI, and **reportingconfig -> domain -> tld** in the Security Management appliance CLI.

To create a Domain-Based Executive Summary report:

---

**Step 1** On the Security Management appliance, you can schedule the report or generate the report immediately.

To schedule the report:

- a. Choose **Email > Reporting > Scheduled Reports**.
- b. Click **Add Scheduled Report**.

The Add Scheduled Report page appears.

To create an on-demand report:

- a. Choose **Email > Reporting > Archived Reports**.
- b. Click **Generate Report Now**.

The Generate Report page appears.

**Step 2** From the **Report Type** drop-down list, choose **Domain-Based Executive Summary** report type.

**Figure 4-28 Adding a Domain-Based Executive Summary Report****Add Scheduled Report**

| Report Settings        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type:                  | Domain-Based Executive Summary <small>Domain-Based reports are not archived</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Title:                 | Domain-Based Executive Summary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Report Generation:     | <p><input type="radio"/> Generate report by specifying individual domains</p> <p>Domain(s): <input type="text"/><br/><small>Separate multiple domains with commas</small></p> <p>Email to: <input type="text"/><br/><small>Separate multiple addresses with commas</small></p> <p><input checked="" type="radio"/> Generate reports by uploading file <small>?</small></p> <p><input checked="" type="radio"/> Select file from configuration directory <small>?</small></p> <div> GLBA-Dictionary.txt<br/> HIPAA-Dictionary.txt<br/> PCI-Dictionary.txt<br/> README<br/> SOX-Dictionary.txt<br/> config.dtd<br/> profanity.txt<br/> proprietary_content.txt<br/> sexual_content.txt </div> <p><input type="radio"/> Select file from local computer <input type="button" value="Browse..."/></p> |
| Outgoing Domain:       | Select the domain type for the outgoing mail summary:<br><input checked="" type="radio"/> By Server<br><input type="radio"/> By Email Address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Time Range To Include: | Previous 7 calendar days                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Format:                | <input checked="" type="radio"/> PDF <small>Preview PDF Report <small>?</small></small><br><input type="radio"/> CSV <small>?</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Schedule:              | <input type="radio"/> Daily At time: 01 : 00<br><input checked="" type="radio"/> Weekly on Sunday<br><input type="radio"/> Monthly on first day of month                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Report Language:       | English/United States [en-us]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Custom Logo:           | <p>Current logo:  <b>IRONPORT®</b></p> <p><input checked="" type="radio"/> Use IronPort logo<br/> <input type="radio"/> Upload a logo <input type="button" value="Browse..."/></p> <p><small>Maximum size 550w x 160h pixels</small></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

- Step 3** Specify the domains to include in the report and the email addresses for the report recipients. You can select one of the following options for generating the report:
- **Generate report by specifying individual domains.** Enter the domains for the report and the email addresses for the report recipients. Use commas to separate multiple entries. You can also use subdomains, such

as subdomain.yourdomain.com. Specifying individual domains is recommended if you create reports for a small number of domains that are not expected to change frequently.

- **Generate reports by uploading file.** Import a configuration file that contains a list of the domains and recipient email addresses for the report. You can select a configuration file from the configuration directory on the appliance or upload one from your local computer. Using a configuration file is recommended if you create reports for a large number of domains that change frequently. For more information on configuration files for domain-based reports, see [Domain-Based Executive Summary Report Configuration Files](#), page 4-72.



#### Note

If you send reports to an external account (such as Yahoo! Mail or Gmail), you may need to add the reporting return address to the external account's whitelist to prevent report messages from being incorrectly classified as spam.

- Step 4** In the Title text field, type the name of the 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 5** In the Outgoing Domain section, choose the domain type for the outgoing mail summary. Choices are: By Server or By Email Address.
- Step 6** From the Time Range to Include drop-down list, select a time range for the report data.
- Step 7** In the Format section, choose the format of the report.
- Choices include:
- **PDF.** Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.
  - **CSV.** Create an ASCII text file that contains the tabular data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.
- Step 8** From the Schedule section, choose a schedule for generating the report.

Choices include: Daily, Weekly (drop-down list for day of week included), or monthly.

- Step 9** (Optional) Upload a custom logo for the report. The logo appears at the top of the report.
- 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 logo is used.
- Step 10** Select a language for this report. For generating PDFs in Asian languages, see important information at [Printing and Exporting Report Data, page 3-20](#).
- Step 11** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- 

## Domain-Based Executive Summary Report Configuration Files

You can use a configuration file to manage the domains and recipients for a Domain-Based Executive Summary report. The configuration file is a text file that is stored in the configuration directory of the appliance. Each line in the file produces a separate report. This allows you to include a large number of domains and recipients in a single report, as well as define multiple domain reports in a single configuration file.

Each line of the configuration file includes a space-separated list of domain names and a space-separated list of email addresses for the report recipients. A comma separates the list of domain names from the list of email addresses. You can include subdomains by appending the subdomain name and a period at the beginning of the parent domain name, such as subdomain.example.com.

The following is a Single Report configuration file that generates three reports.

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```



### Note

You can use a configuration file and the settings defined for a single named report to generate multiple reports at the same time. For example, a company named Bigfish purchases two other companies, Redfish and Bluefish, and continues to maintain their domains. Bigfish creates a single Domain-Based Executive Summary report using a configuration file containing three lines corresponding to separate domain reports. When the appliance generates a Domain-Based

Executive Summary report, an administrator for Bigfish receives a report on the Bigfish.com, Redfish.com, and Bluefish.com domains, while a Redfish administrator receives a report on the Redfish.com domain and a Bluefish administrator receives a report on the Bluefish.com domain.

---

You can upload a different configuration file to the appliance for each named report. You can also use the same configuration file for multiple reports. For example, you might create separate named reports that provide data about the same domains over different time periods. If you update a configuration file on your appliance, you do not have to update the report settings in the GUI unless you change the filename.

## Executive Summary Reports

The Executive Summary Report is a high-level overview of the incoming and outgoing email message activity from your Email Security appliances. that can be viewed on the Security Management appliance.

This report page summarizes what you can view on the [Email Reporting Overview Page](#). For more information on the Email Reporting Overview page, see “[Email Reporting Overview Page](#)” section on page 4-12.

## Generating Reports On Demand

In addition to the reports that you can view (and generate PDFs for) using the interactive report pages described in [Understanding the Email Reporting Pages, page 4-11](#), you can generate PDF or CSV files for the reports listed in [About Scheduled and On-Demand Reports, page 4-66](#) at any time, for the time frame that you specify.

To generate an on-demand report perform the following:

- 
- Step 1** On the Security Management appliance, choose **Email > Reporting > Archived Reports**.
  - Step 2** Click **Generate Report Now**.  
The Generate Report page appears.

**Figure 4-29 Generate Report Page****Generate Report**

| Generate Report                                                                   |                                                                                                                                                                             |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Report Type:                                                                      | Select report type... ▼                                                                                                                                                     |
| Title:                                                                            | <input type="text"/>                                                                                                                                                        |
| Time Range To Include:                                                            | Previous 7 calendar days ▼                                                                                                                                                  |
| Format:                                                                           | <input checked="" type="radio"/> PDF<br><input type="radio"/> CSV ?                                                                                                         |
| Delivery Options:                                                                 | <input checked="" type="checkbox"/> Archive<br><input type="checkbox"/> Email now to recipients:<br><input type="text"/><br><i>Separate multiple addresses with commas.</i> |
| Report Language:                                                                  | English/United States [en-us] ▼                                                                                                                                             |
| <a href="#">&lt; Back to Archived Reports</a> <a href="#">Deliver This Report</a> |                                                                                                                                                                             |

**Step 3** From the Report type section, choose a report type from the drop-down list.

For descriptions of the report types, see [About Scheduled and On-Demand Reports, page 4-66](#).

**Step 4** In the Title text field, type the name of the 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.

**Note**

For information about the settings for a Domain-Based Executive Summary report, see [Domain-Based Executive Summary Report, page 4-68](#).

**Note**

Available options for scheduled reports differ by report type. Options described in the remainder of this procedure do not necessarily apply to all reports.

**Step 5** From the Time Range to Include drop-down list, select a time range for the report data. (This option is not available for Virus Outbreak reports.)

Note the custom time range option.



**Step 6** In the Format section, choose the format of the report.

Choices include:

- **PDF.** Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.
- **CSV.** Create an ASCII text file that contains the tabular data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.

**Step 7** Select the appliances or appliance groups for which you want to run the report. If you have not created any appliance groups, this option does not appear.

**Step 8** From the Delivery Option section, choose the following:

- Archive the report by checking the **Archive Report** checkbox.
- By choosing this, the report will be listed on the Archived Reports page.




---

**Note** Domain-Based Executive Summary reports cannot be archived.

---

- Email the report, by checking the **Email now to recipients** checkbox.

In the text field, type in the recipient email addresses for the report.

**Step 9** Select a language for this report. For generating PDFs in Asian languages, see important information at [Printing and Exporting Report Data, page 3-20](#).

**Step 10** Click **Deliver This Report** to generate the report.

---

## Scheduled Reports

You can schedule any of the reports listed in [About Scheduled and On-Demand Reports, page 4-66](#).

To manage report scheduling, see the following:

- [Adding Scheduled Reports, page 4-76](#)
- [Editing Scheduled Reports, page 4-77](#)

- [Discontinuing Scheduled Reports, page 4-78](#)

## Adding Scheduled Reports

To add a scheduled email report, use the following steps:

**Step 1** On the Security Management appliance window, choose **Email > Reporting > Scheduled Reports**.

**Step 2** Click **Add Scheduled Report**.

The Add Scheduled Report page appears.

**Figure 4-30** *Add Scheduled Reports Page*  
**Add Scheduled Report**

The screenshot shows the 'Add Scheduled Report' page with the following settings:

- Report Settings** (Section Header)
- Type:** Select report type... (Dropdown menu)
- Title:** (Text input field)
- Time Range To Include:** Previous 7 calendar days (Dropdown menu)
- Format:**
  - ☒ PDF
  - ☐ CSV ?
- Schedule:**
  - ☐ Daily
  - ☒ Weekly on Sunday (Dropdown menu)
  - ☐ Monthly on first day of month
- At time:** 01 : 00 (Time selection)
- Email to:** (Text input field with placeholder: Separate multiple addresses with commas. Leave blank for archive only.)
- Report Language:** English/United States [en-us] (Dropdown menu)
- Buttons:** Cancel, Submit

**Step 3** From drop-down menu next to **Type**, choose your report type.

For descriptions of the report types, see [About Scheduled and On-Demand Reports, page 4-66](#).



### Note

For information about the settings for a Domain-Based Executive Summary report, see [Domain-Based Executive Summary Report, page 4-68](#).



### Note

Available options for scheduled reports differ by report type. Options described in the remainder of this procedure do not necessarily apply to all reports.

- Step 4** In the **Title** field, type the title of your report.
- To avoid creating multiple reports with the same name, we recommend using a descriptive title.
- Step 5** Choose the time range for the report from the **Time Range to Include** drop-down menu. (This option is not available for Virus Outbreak reports.)
- Step 6** Choose the **format** for the generated report.
- The default format is PDF. Most reports allow scheduling of CSV.
- Step 7** Depending on the report, for **Number of Rows**, choose the amount of data to include.
- Step 8** Depending on the report, choose the column by which to sort the report.
- Step 9** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report. Additionally, include the time that you want the report scheduled for. Time increments are based on midnight to midnight (00:00 to 23:59).
- Step 10** In the **Email** text field, type in the email address where the generated report will be sent.
- If you do not specify an email recipient, the system will still archive the reports. You can add as many recipients for reports as you want, including zero recipients. If you need to send the reports to a large number of addresses, however, you may want to create a mailing list instead of listing the recipients individually.
- Step 11** Choose a language for the report.
- For Asian languages, see important information at [Printing and Exporting Report Data, page 3-20](#).
- Step 12** Click **Submit**.
- 

## Editing Scheduled Reports

To edit scheduled reports, perform the following steps:

- 
- Step 1** On the Security Management appliance window, choose **Email > Reporting > Scheduled Reports**.

- Step 2** Click the report name link in the Report Title column that you want to modify. The Edit Scheduled Report page appears.
- Step 3** From the **Edit Scheduled Report** page, modify the report settings.
- Step 4** Click **Submit** to submit your changes on the page, then click the **Commit Changes** button to commit your changes on the appliance.
- 

## Discontinuing Scheduled Reports

To prevent future instances of scheduled reports from being generated, perform the following steps:

- Step 1** On the Security Management appliance window, choose **Email > Reporting > Scheduled Reports**.
- Step 2** Select the check boxes corresponding to the reports that you want to discontinue generating. To remove all scheduled reports, select the **All** check box.
- Step 3** Click **Delete**.



**Note** Any archived versions of deleted reports are *not* automatically deleted. To delete previously-generated reports, see [Deleting Archived Reports, page 4-80](#).

---

## Archived Reports



**Note** For more information about generating a report immediately by clicking **Generate Report Now**, see [Generating Reports On Demand, page 4-73](#).

---

Scheduled and on-demand reports are archived for a period of time.

The Security Management appliance retains the most recent reports that it generates, up to 12 instances of each scheduled report, up to 1000 total versions for all reports. The limit of 12 instances applies to each scheduled report with the same name and time range.

Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000.

Archived reports are stored in the `/periodic_reports` directory on the appliance. (See [Appendix A, “Accessing the Appliance”](#) for more information.)

## Accessing Archived Reports

The **Email > Reporting > Archived Reports** page lists scheduled and on-demand reports that you have chosen to archive which have been generated and not yet purged.

To access archived reports, perform the following:

- 
- Step 1** On the Security Management appliance window, choose, **Email > Reporting > Archived Reports**.

The Archived Reports page appears.

**Figure 4-31**      *Archived Reports*

### Archived Reports

| Available Reports      |                 |          |                 |               |                                | Show: All reports        |
|------------------------|-----------------|----------|-----------------|---------------|--------------------------------|--------------------------|
| Generate Report Now... |                 |          |                 |               |                                |                          |
| Report Title           | Type            | Format ▼ | Appliance/Group | Time Range    | Generated on                   | All                      |
| Content Filters        | Content Filters | PDF      | ALL             | Calendar Week | 09 May 2011 12:31 (GMT -07:00) | <input type="checkbox"/> |
| Delivery Status        | Delivery Status | PDF      | ALL             | Custom        | 09 May 2011 12:32 (GMT -07:00) | <input type="checkbox"/> |
|                        |                 |          |                 |               |                                | Delete                   |

- Step 2** To locate a particular report if the list is long, filter the list by choosing a report type from the **Show** menu, or click a column heading to sort by that column.
- Step 3** Click the Report Title to view that report.
-

## Deleting Archived Reports

Reports are automatically deleted from the system according to the rules outlined in [Archived Reports, page 4-78](#). However, you can manually delete unneeded reports.

To manually delete Archived reports, perform the following:

- 
- |               |                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | On the Security Management appliance, choose <b>Email &gt; Reporting &gt; Archived Reports</b> .                                        |
|               | The Archived reports that are available are displayed.                                                                                  |
| <b>Step 2</b> | Select the checkbox for one or more reports to delete.                                                                                  |
| <b>Step 3</b> | Click <b>Delete</b> .                                                                                                                   |
| <b>Step 4</b> | To prevent future instances of scheduled reports from being generated, see <a href="#">Discontinuing Scheduled Reports, page 4-78</a> . |
-



## CHAPTER 5

# Using Centralized Web Reporting

---

This chapter contains the following sections:

- [Reporting Overview, page 5-1](#)
- [Getting Started with Web Reporting, page 5-3](#)
- [Configuring Centralized Web Reporting, page 5-3](#)
- [Using the Web Reporting Tab, page 5-5](#)
- [Understanding the Web Reporting Pages, page 5-11](#)
- [Scheduling Reports, page 5-82](#)
- [Archiving Reports, page 5-89](#)

## Reporting Overview

The Web reporting functionality aggregates information from individual security features and records data that can be used to monitor your web traffic patterns and security risks. You can run reports in real-time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals. Reporting functionality also allows you to export raw data to a file.

The Centralized Web Reporting feature not only generates high-level reports, allowing administrators to understand what is happening on their network, but it also allows an administrator to drill down and see traffic details for a particular domain, user, or category.

## Domain Information

For a domain, the web reporting feature can generate the following data elements to be on a domain report. For example, if you are generating a report on the Facebook.com domain, the report may contain:

- A list of the top users who accessed Facebook.com
- A list of the top URLs that were accessed within Facebook.com

## User

For a user, the web reporting feature can generate data elements to be on a user report. For example, for the user report titled ‘Jamie’, the report may contain:

- A list of the top domains that the user ‘Jamie’ accessed
- A list of the top URLs that were malware or virus positive
- A list of the top categories that the user ‘Jamie’ accessed

## Category

For a category, the web reporting feature can generate data to be included in a category report. For example, for the category ‘Sports’, the report may contain:

- A list of the top domains that were in the ‘Sports’ category
- A list of the top users who accessed the ‘Sports’ category

In all of these examples, these reports are intended to give a comprehensive view about a particular item on the network so that the administrator can take action.

For a detailed description on logging pages versus reporting pages, see the [“Logging Versus Reporting” section on page 13-2](#).



### Note

It is important to remember that web reporting allows you to retrieve all the domain information that a user goes to, not necessarily the specific URL that is accessed. For information on a specific URL that the user is accessing, what time they went to that URL, whether that URL is allowed, etc., use the Web Tracking feature discussed in this chapter.



# Getting Started with Web Reporting



## Note

Before you can view web reporting for the Web Security appliances, you must add and configure the Web Security appliance. For information on adding a Web Security appliance, see the [“Adding Managed Appliances” section on page 3-10](#); for information on the configuration settings for these appliances, see the *Cisco IronPort AsyncOS 7.1 for Web User Guide*.

There are several ways that you can view web reporting data on the Security Management appliance. To get started on web reporting, use the following steps:

- To enable web reporting, see [Configuring Centralized Web Reporting, page 5-3](#)
- To view and manage the various interactive report pages, see [Understanding the Web Reporting Pages, page 5-11](#).
- To create scheduled reports that run on a daily, weekly, or monthly basis, see [Scheduling Reports, page 5-82](#).
- To view archived versions of previously run reports (both scheduled and Generate Report Now), see [Archiving Reports, page 5-89](#).

## Configuring Centralized Web Reporting

Before you use web reporting on the Security Management appliance, you must configure the Security Management appliance to enable all web reporting. Additionally, you can choose to make usernames unrecognizable in all reports.

To configure the settings for centralized web reporting:

- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.

The Centralized Web Reporting page appears. If you are enabling centralized reporting for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.

- Step 2** Click **Edit Settings**.

**Step 3** The Edit Centralized Web Reporting Service Settings page appears.

Logged in as: **admin** on **vmw002-esa03.run**  
Options ▾ Help and Support ▾

Management Appliance | Email | Web

Centralized Services | Network | System Administration

**Edit Centralized Web Reporting Service Settings** Commit Changes >

Web Reporting Service

☒ **Enable Centralized Web Reporting Service**

Username in Reports: ☐ Anonymize usernames in reports

*If you turn off this service you will not be able to use the Centralized Web Reporting feature.*

Cancel Submit

**Step 4** Click the **Enable Centralized Web Report Services** checkbox.

The Web Security appliance only stores data if local reporting is used. If centralized reporting is enabled for the Web Security appliance then the Web Security appliance does NOT retain any reporting data except for System Capacity and System Status. If Centralized Web Reporting is not enabled, the only reports that are generated are System Status and System Capacity.

**Step 5** To generate reports so that user names are unrecognizable in scheduled reports, check the **Anonymize usernames in reports** checkbox. The default setting is that all usernames appear in scheduled reports.



**Note**

If you have administrator status, you will always see the user names.

**Step 6** Click **Submit** to submit your changes, then click the **Commit Changes** to commit your changes on the appliance.



**Note**

If you have enabled web reporting on the appliance, and there is no disk space allocated for this action, centralized web reporting will not work until disk space is allocated. As long as the quota you are setting the Web Reporting and Tracking to is larger than the currently used disk space, you will not lose any Web Reporting and Tracking data. See the [“Managing Disk Usage” section on page 12-115](#), for more information.

# Using the Web Reporting Tab

The **Web > Reporting** tab provides several options for viewing reporting data. This section describes each of the reporting pages under this tab, and explains the information displayed on each of the reporting pages.

**Note**

---

For information on which one of these categories on the Web Reporting tab can generate scheduled reports, see the [“Scheduling Reports” section on page 5-82](#).

---

**Table 5-1 Web Reporting Tab Details**

| Web Reporting Menu                          | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Web Reporting Overview Page</a> | The Overview page provides a synopsis of the activity on your Cisco IronPort appliances. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the <a href="#">“Web Reporting Overview Page” section on page 5-12.</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <a href="#">Users Page</a>                  | <p>The Users page provides several web tracking links that allows you to view web tracking information for individual users.</p> <p>From the <b>Users</b> page you can view how long a user, or users, on your system have spent on the internet, on a particular site or URL, and how much bandwidth that user is using.</p> <p>From the <b>Users</b> page you can click on an individual user in the interactive Users table to view more details for that specific user on the User Details page.</p> <p>The <b>User Details</b> page allows you to see specific information about a user that you have identified in the Users table on the <b>Web &gt; Reporting &gt; Users</b> page. From this page you can investigate individual user’s activity on your system. This page is particularly useful if you are running user-level investigations and need to find out, for example, what sites your users are visiting, what Malware threats they are encountering, what URL categories they are accessing, and how much time a specific user is spending at these sites.</p> <p>For more information, see the <a href="#">“Users Page” section on page 5-16.</a> For information on a specific user in your system, see the <a href="#">“User Details Page” section on page 5-20</a></p> |
| <a href="#">Web Sites Page</a>              | The Web Sites page allows you to view an overall aggregation of the activity that is happening on your managed appliances. From this page you can monitor high-risk web sites accessed during a specific time range. For more information, see the <a href="#">“Web Sites Page” section on page 5-24.</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 5-1      Web Reporting Tab Details**

| Web Reporting Menu                 | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URL Categories Page</b>         | <p>The URL Categories page allows you to view the top URL Categories that are being visited on the site including:</p> <ul style="list-style-type: none"> <li>the top URLs that have triggered a block or warning action to occur per transaction.</li> <li>all the URL categories during a specified time range for both completed, warned and blocked transactions. This is an interactive table with interactive column headings that you can use to sort data as you need.</li> </ul> <p>From this page you can also create, edit or delete a custom URL category. For more information, see the <a href="#">“URL Categories Page” section on page 5-28</a>.</p> |
| <b>Application Visibility Page</b> | <p>The Application Visibility page allows you to apply and view the controls that have been applied to a particular application types within the Security Management appliance and Web Security appliance. For more information, see the <a href="#">“Application Visibility Page” section on page 5-36</a>.</p>                                                                                                                                                                                                                                                                                                                                                     |
| <b>Security</b>                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Anti-Malware Page</b>           | <p>The Anti-Malware page allows you to view information about malware ports and malware sites that the L4 Traffic Monitor detected during the specified time range. The upper part of the report displays the number of connections for each of the top malware ports and web sites. The lower part of the report displays malware ports and sites detected. For more information, see the <a href="#">“Anti-Malware Page” section on page 5-41</a>.</p>                                                                                                                                                                                                             |

**Table 5-1 Web Reporting Tab Details**

| Web Reporting Menu                   | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client Malware Risk Page</b>      | <p>The Client Malware Risk page is a security-related reporting page that can be used to monitor client malware risk activity.</p> <p>From the Client Malware Risk page, a system administrator can see which of their users are encountering the most blocks or warnings. Given the information gathered from this page, the administrator can click on the user link to view what this user doing on the web that makes them run into so many blocks or warnings and setting off more detections than the rest of the users on the network.</p> <p>For more information, see the <a href="#">“Client Malware Risk Page” section on page 5-50.</a></p> |
| <b>Web Reputation Filters Page</b>   | <p>Allows you to view reporting on Web Reputation filtering for transactions during a specified time range. For more information, see the <a href="#">“Web Reputation Filters Page” section on page 5-57.</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>L4 Traffic Monitor Data Page</b>  | <p>Allows you to view information about malware ports and malware sites that the L4 Traffic Monitor detected during the specified time range. For more information, see the <a href="#">“L4 Traffic Monitor Data Page” section on page 5-63.</a></p>                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Reports by User Location Page</b> | <p>The Reports by User Location page allows you to find out what activities that your mobile users are conducting from their local or remote systems.</p> <p>For more information, see the <a href="#">“Reports by User Location Page” section on page 5-66.</a></p>                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Reporting</b>                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Table 5-1**      **Web Reporting Tab Details**

| Web Reporting Menu            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web Tracking Page</b>      | <p>The Web Tracking page allows you to track and see basic web-related information such as the type of web traffic that is being handled by the appliances.</p> <p>This includes information such as time ranges, and UserID and Client IP addresses, but also includes information like certain types of URLs, how much bandwidth that each connection is taking up, or tracking a specific user's web usage.</p> <p>For more information, see the <a href="#">“Web Tracking Page” section on page 5-69</a>.</p> |
| <b>System Capacity Page</b>   | <p>Allows you to view the overall workload that is sending reporting data to the Security Management appliance.</p> <p>For more information, see the <a href="#">“System Capacity Page” section on page 5-74</a>.</p>                                                                                                                                                                                                                                                                                             |
| <b>Data Availability Page</b> | <p>Allows you to get a glimpse of the impact of the reporting data on the Security Management appliance for each appliance.</p> <p>For more information, see the <a href="#">“Data Availability Page” section on page 5-80</a>.</p>                                                                                                                                                                                                                                                                               |
| <b>Scheduling Reports</b>     | <p>Allows you to schedule reports for a specified time range. For more information, see the <a href="#">“Scheduling Reports” section on page 5-82</a>.</p>                                                                                                                                                                                                                                                                                                                                                        |
| <b>Archiving Reports</b>      | <p>Allows you to archive reports for a specified time range. For more information, see the <a href="#">“Archiving Reports” section on page 5-89</a>.</p>                                                                                                                                                                                                                                                                                                                                                          |

**Note**

You can schedule reports for most of the web reporting categories, including additional reports for Extended Top URL Categories and Top Application Types. For more information on scheduling reports, see the [“Scheduling Reports” section on page 5-82](#).

## Interactive Report Pages for the Web Security Appliance

All of the Web reporting pages are interactive report pages. This allows you to monitor information on one or all of the managed Web Security appliances in your system.

With the interactive report pages, you can view centralized reporting for different time ranges, and specify what interactive column types you want to view on each page. Many of the report pages have interactive columns that can be configured to sort the data in each column specific to your needs for viewing data on that page. For information on configuring interactive columns on your report pages, see the [“Configuring Column Settings on Report Pages” section on page 5-10](#).



### Note

Not every column is available for every report page. Click on the **‘Column’** link for each reporting page to view the columns available for that specific report page. The [“Interactive Columns for the Centralized Web Reporting Pages” section on page E-1](#) describes the columns available on the reporting pages in this release.

Additionally, one of the possible results that the column provides is a link to the [Web Tracking Page](#) for that result.

For information on configuring time ranges on the reporting pages, see the [“Choosing a Time Range for Interactive Reports” section on page 3-18](#).

## Configuring Column Settings on Report Pages

To configure column settings on your report pages, perform the following steps:

- Step 1** On the Security Management appliance page, choose **Web > Reporting > Your\_Web\_Reporting\_Page**.
- Step 2** Click **Columns**.  
A pop-up window appears and allows you to select the columns that you want to appear.
- Step 3** Click on the checkbox next to each category in the pop-up window. Once you have selected the options, choose **Done**. The interactive column headings can now be used to sort the data in each column specific to your needs.



**Note**

A link to web tracking details is provided for several of the columns on each report page.

## Printing Reports from Report Pages

You can generate a printer-friendly formatted PDF version of any of the report pages by clicking the Printable PDF link at the top-right of the page. You can export graphs and other data to comma-separated values (CSV) format by clicking the Export link. Most reports allow scheduling of CSV formatting. However, you cannot schedule an extended report with a CSV format.

For more information on printing from report pages, see the [“Printing and Exporting Report Data” section on page 3-20](#)

Export links that are visible on each page, are used to export raw data.

## Reporting Filters for Report Pages

AsyncOS provides reporting filters that allow you to restrict the aggregation of data in reports that cover the previous year (Last Year reports). You can use these filters if the performance of aggregated reporting decreases due to a large number of unique entries over the course of a month. These filters can restrict detailed, individual IP, domain, or user data in reports. Overview reports and summary information remain available for all reports.

For more information on how to enable reporting filters, see [“Reporting Filters on the Security Management Appliance” section on page 3-19](#).

## Understanding the Web Reporting Pages

This section discusses the various report pages that are used by the Security Management appliance for Web Reporting.

They include:

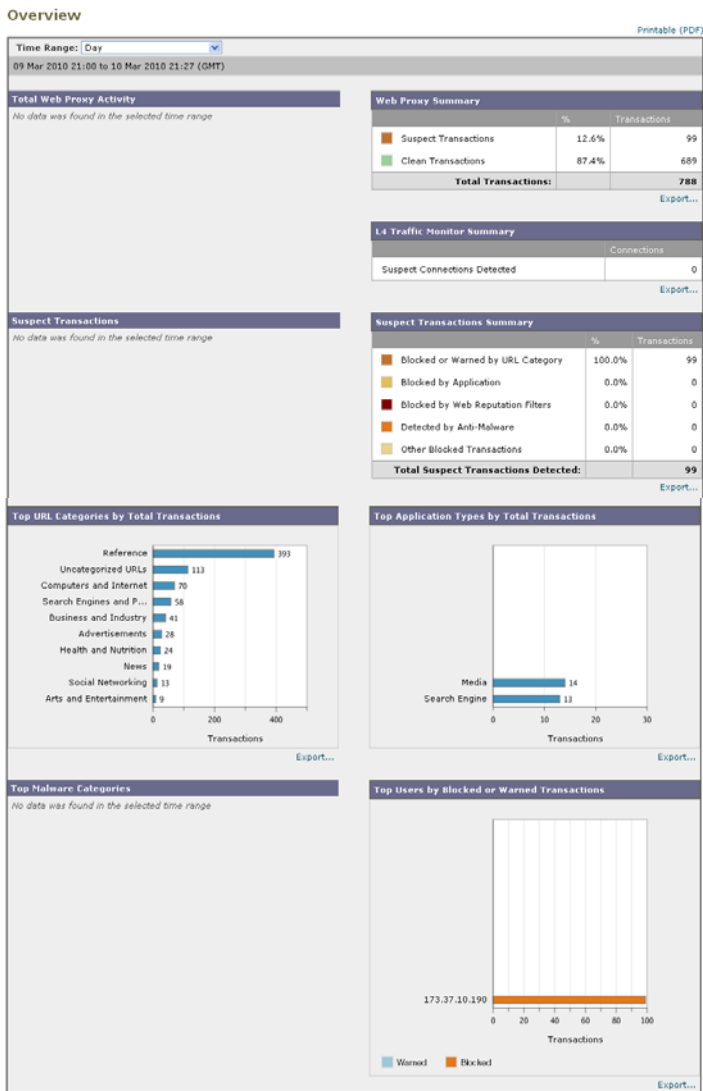
- [Web Reporting Overview Page](#), page 5-12
- [Users Page](#), page 5-16
- [User Details Page](#), page 5-20
- [Web Sites Page](#), page 5-24
- [URL Categories Page](#), page 5-28
- [Application Visibility Page](#), page 5-36
- [Anti-Malware Page](#), page 5-41
- [Client Malware Risk Page](#), page 5-50
- [Web Reputation Filters Page](#), page 5-57
- [L4 Traffic Monitor Data Page](#), page 5-63
- [Reports by User Location Page](#), page 5-66
- [Web Tracking Page](#), page 5-69
- [System Capacity Page](#), page 5-74
- [Data Availability Page](#), page 5-80

## Web Reporting Overview Page

The **Web > Reporting > Overview** page provides a synopsis of the activity on your Cisco IronPort appliances. It includes graphs and summary tables for the incoming and outgoing transactions.

[Figure 5-1](#) shows the Overview page.

Figure 5-1 The Web &gt; Reporting &gt; Overview Page



At a high level the **Overview** page shows you statistics about the URL and User usage, Web Proxy activity, and various transaction summaries. The transaction summaries gives you further trending details on, for example suspect transactions, and right across from this graph, how many of those suspect transactions are blocked and in what manner they are being blocked.

The lower half of the **Overview** page is about usage. That is, the top URL categories being viewed, the top application types and categories that are being blocked, and the top users that are generating these blocks or warnings.

The following list explains the various sections on the **Overview** page:

**Table 5-2**      ***Details on the Web > Reporting > Overview Page***

| Section                            | Description                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b> | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                 |
| <b>Total Web Proxy Activity</b>    | This section allows you to view the web proxy activity that is being reported by the Web Security appliances that are currently managed by the Security Management appliance.<br><br>This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline). |
| <b>Web Proxy Summary</b>           | This section allows you to view the percentage of web proxy activity that are suspect, or clean proxy activity, including the total number of transactions.                                                                                                                                                                                     |
| <b>L4 Traffic Monitor Summary</b>  | This section reports any Layer 4 traffic that is being reported by the Web Security appliances that are currently managed by the Security Management appliance.                                                                                                                                                                                 |
| <b>Suspect Transactions</b>        | This section allows you to view the web transactions that have been labeled as suspect by the administrator.<br><br>This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).                                                                  |

**Table 5-2**      *Details on the Web > Reporting > Overview Page*

| Section                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Suspect Transactions Summary</b>                | This section allows you to view the percentage of blocked or warned transactions that are suspect. Additionally you can see the type of transactions that have been detected and blocked, and the actual number of times that this transaction was blocked.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Top URL Categories by Total Transactions</b>    | This section displays the top 10 URL categories that are being blocked, including the type of URL category (vertical scale) and the actual number of times the specific type of category has been blocked (horizontal scale).                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Top Application Types by Total Transactions</b> | This section displays the top application types that are being blocked, including the name of the actual application type (vertical scale) and the number of times the specific application has been blocked (horizontal scale).                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Top Malware Categories Detected</b>             | This section displays all Malware categories that have been detected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Top Users Blocked or Warned Transactions</b>    | This section displays the actual users that are generating the blocked or warned transactions. Users can be displayed by IP address, or by user name. The user name or IP address can be made unrecognizable for reporting purposes. For more information on how to make user names unrecognizable in for this page or in scheduled reports, see the section <a href="#">“Configuring Centralized Web Reporting”</a> section on page 5-3. The default setting is that all usernames appear. For an example of how to do this, see <a href="#">“Example 4: Privacy and Hiding User Names”</a> section on page D-12. |

From the **Overview** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Printing Reports from Report Pages”](#) section on page 5-11.

**Note**

You can generate a scheduled report for Users. See the [“Scheduling Reports”](#) section on page 5-82.

# Users Page

The **Web > Reporting > Users** page provides several links that allows you to view web reporting information for individual users.

From the **Users** page you can view how long a user, or users, on your system have spent on the internet, on a particular site or URL, and how much bandwidth that user is using.



---

**Note**

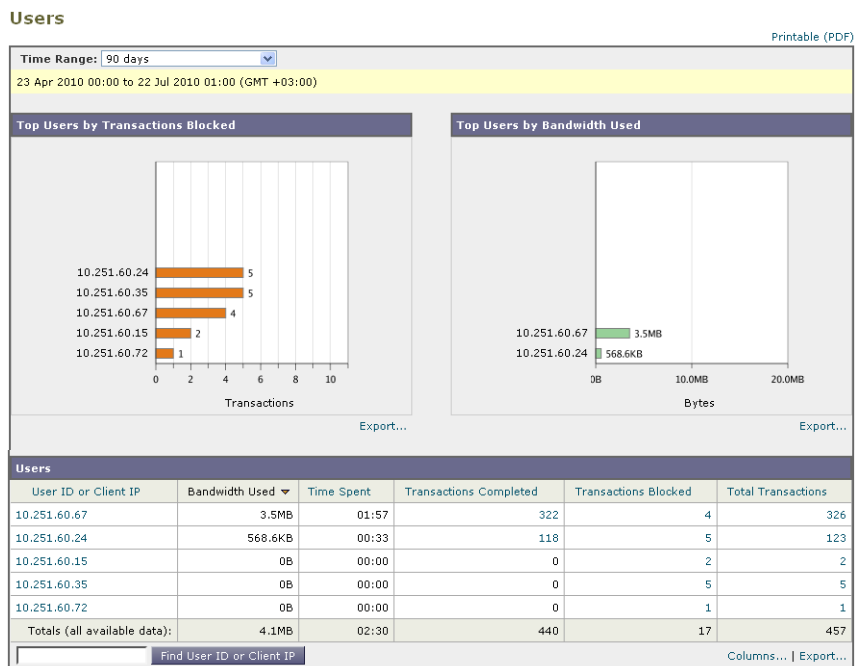
The maximum number of users on the Web Security appliance that the Security Management appliance can support is 500.

---

To access the Users page, perform the following:

- 
- Step 1** On the Security Management appliance window, choose **Web > Reporting > Users**.

The **Users** page appears.

**Figure 5-2 Web > Reporting > Users Page**

From the **Users** page, you can view the following information pertaining to the users on your system:

**Table 5-3**      *Details on the Web > Reporting > Users Page*

| Section                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Range (drop-down list)       | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Top Users by Transactions Blocked | This section lists the top users, by either IP address or user name (vertical scale), and the number of transactions that have been blocked specific to that user (horizontal scale). The user name or IP address can be made unrecognizable for reporting purposes. For more information on how to make user names unrecognizable in for this page or in scheduled reports, see the section <a href="#">“Configuring Centralized Web Reporting”</a> section on page 5-3. The default setting is that all usernames appear. For an example of how to do this, see <a href="#">“Example 4: Privacy and Hiding User Names”</a> section on page D-12. |



**Table 5-3**      *Details on the Web > Reporting > Users Page*

| Section                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Top Users by Bandwidth Used</b> | This sections displays the top users, by either IP address or user name (vertical scale), that are using the most bandwidth on the system (horizontal scale represented in gigabyte usage).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Users Table</b>                 | <p>The Users table is an interactive table where you can sort the user information in a myriad of ways to get a different look and feel each time you view the table. The information in each column can be sorted from ascending to descending order, by clicking on the column heading.</p> <p>The columns represented in this table are customizable. For information on configuring columns for the Users table, see the <a href="#">“Interactive Report Pages for the Web Security Appliance”</a> section on page 5-10.</p> <p>After you have selected the column categories that you want to appear in the interactive Users table, you can select how many items you want to be displayed from the <b>Items Displayed</b> drop-down menu; choices are: 10, 20, 50, or 100.</p> <p>Additionally, you can find a specific User ID or Client IP address. In the text field at the bottom of the User section, enter the specific User ID or Client IP address and click on <b>Find User ID or Client IP Address</b>. The IP address does not need to be an exact match to return results.</p> <p>From the Users table you can click on a specific user to find more specific information. This information appears on the User Details page. For more information on the User Details page, see the <a href="#">“User Details Page”</a> section on page 5-20</p> |

**Note**

**You cannot add or delete users from this page.**

For more information on adding or deleting a user, see the [“Managing Users with the GUI”](#) section on page 12-55. For more information on user roles themselves, see the [“User Roles”](#) section on page 12-40, and [Table 12-2](#) on page 12-40. For information on customizing the user’s role, see the [“Creating Custom Web User Roles”](#) section on page 12-52.

**Note**

You need to configure LDAP authentication to view client user IDs instead of client IP addresses. Without LDAP authentication the system can only refer to users by their IP address.

Set up LDAP authentication on the Security Management appliance by choosing **Management Appliance > System Administration > LDAP > Add LDAP Server Profile**. Choose the **Use Password** radio button, and enter the User name and password. By doing this, the user name will now be seen on the Users and User Details page.

From the **Users** page you can also print or export the print PDF to a CSV file. For information on printing or exporting a file, see the [“Printing Reports from Report Pages” section on page 5-11](#). You can also generate a scheduled report for Users. See the [“Scheduling Reports” section on page 5-82](#).

**Note**

User information within a scheduled report for this page can be made to be unrecognizable. For information on making user information unrecognizable, see the [“Enabling and Disabling Centralized Web Reporting on a Security Management Appliance” section on page 3-5](#).

To view an example of how the **Users** page may be used, see [“Example 1: Investigating a User” section on page D-2](#).

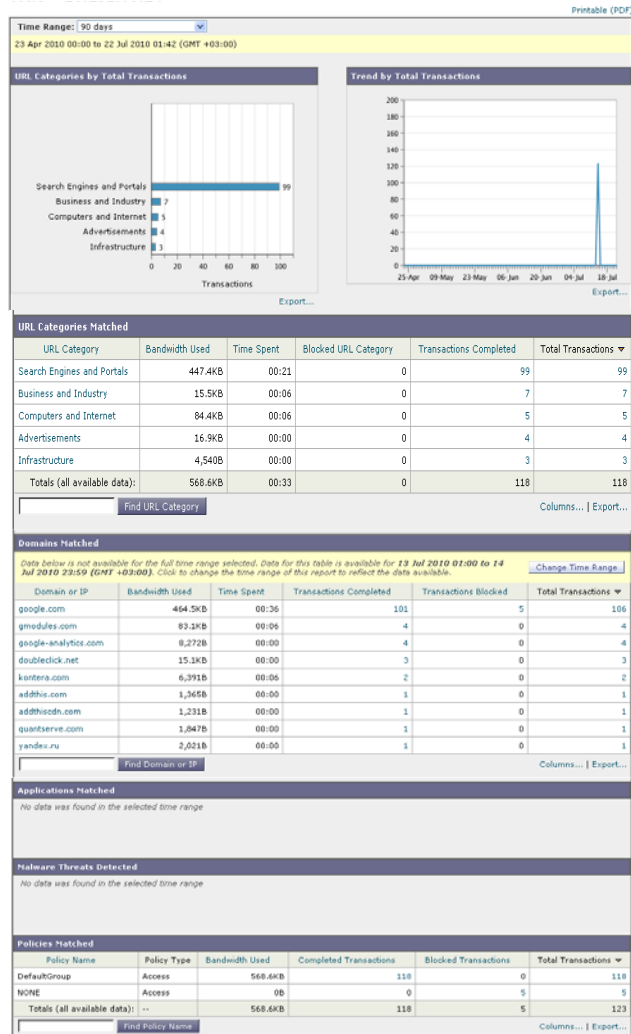
## User Details Page

The **User Details** page allows you to see specific information about a user that you have identified in the interactive Users table on the **Web > Reporting > Users** page.

The **User Details** page allows you to investigate individual user’s activity on your system. This page is particularly useful if you are running user-level investigations and need to find out, for example, what sites your users are visiting, what Malware threats they are encountering, what URL categories they are accessing, and how much time a specific user is spending at these sites.

To display the **User Details** page for a specific user, click on a specific user from the User table on the **Web > Users** page and the following page appears:

Figure 5-3 User Details Page



From the **User Details** page, you can view the following information pertaining to an individual user on your system:

**Table 5-4**      *Details on the Web > Reporting > User > User Details Page*

| Section                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>          | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                                                                                                                 |
| <b>URL Categories by Total Transactions</b> | This section lists the specific URL Categories that a specific user is using.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Trend by Total Transaction</b>           | <p>This graph indicates the trend of a specific users web transactions over time. In essence, when was this specific user on the web and at what times were they out browsing traffic.</p> <p>For example, this graph will indicate if there is a large spike in web traffic during certain hours of the day, and when those spikes occur. Using the Time Range drop-down list, you can expand this graph to see a more or less granular span of time that this user was on the web.</p>                                        |
| <b>URL Categories Matched</b>               | <p>The URL Categories Matched section shows all matched categories during a specified time range for both completed and blocked transactions. You can use interactive column headings to sort data, and the Items Displayed menu changes the number of URL categories displayed in the list.</p> <p>From this section you can also find a specific URL Category. In the text field at the bottom of the section enter the URL Category and click <b>Find URL Category</b>. The category does not need to be an exact match.</p> |
| <b>Domains Matched</b>                      | From this section you can find out about a specific Domain or IP address that this user has accessed. You can also see the time spent on those categories, and various other information that you have set from the column view. In the text field at the bottom of the section enter the Domain or IP address and click <b>Find Domain or IP</b> . The domain or IP address does not need to be an exact match.                                                                                                                |

**Table 5-4**      *Details on the Web > Reporting > User > User Details Page*

| Section                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Applications Matched</b>     | <p>From this section you can find a specific application that a specific user is using. For example, if a user is accessing a site that requires use of a lot of Flash video, you will see the application type in the Application column.</p> <p>In the text field at the bottom of the section enter the application name and click <b>Find Application</b>. The name of the application does not need to be an exact match.</p> |
| <b>Malware Threats Detected</b> | <p>From this table you can see the top Malware threats that a specific user is triggering. In the text field at the bottom of the Malware Threats section, enter the Malware Threat name and click <b>Find Malware Threat</b>. The name of the Malware Threat does not need to be an exact match.</p>                                                                                                                              |
| <b>Policies Matched</b>         | <p>From this section you can find a specific policy that is being enforced on this particular user.</p> <p>In the text field at the bottom of the section enter the policy name and click <b>Find Policy</b>. The name of the policy does not need to be an exact match.</p>                                                                                                                                                       |

You can configure the columns that you want to appear in several sections on the **User Details** page. For information on configuring columns, see the [“Interactive Report Pages for the Web Security Appliance”](#) section on page 5-10.

After you have selected the categories that you want to appear in the interactive sections, you can select how many items you want to be displayed from the Items Displayed drop-down menu. Choices are: 10, 20, 50, or 100.

To view an example of how the User Details page may be used, see [“Example 1: Investigating a User”](#) section on page D-2.

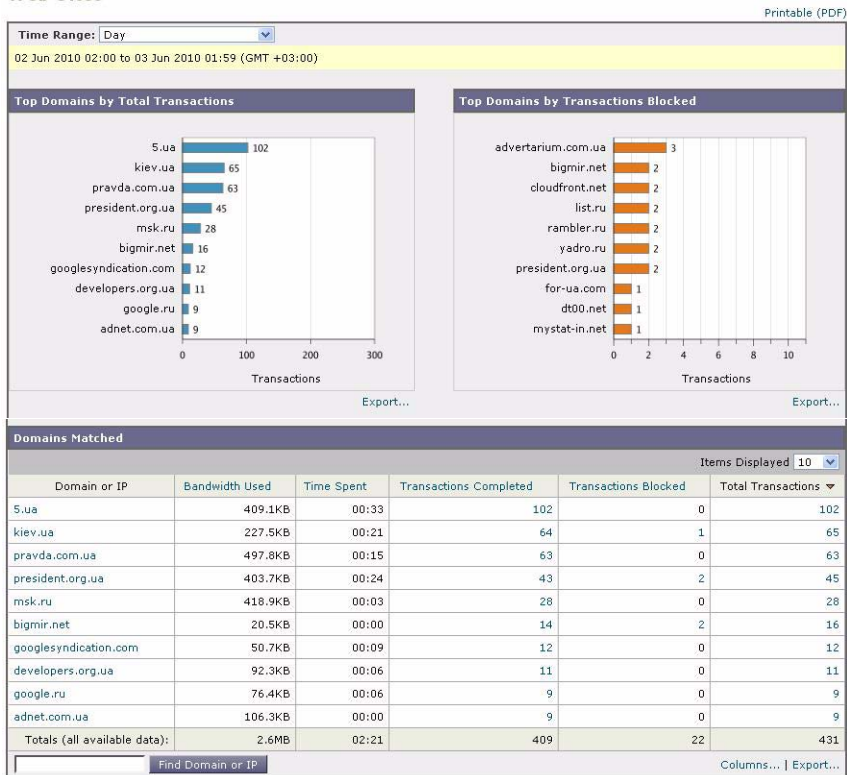
# Web Sites Page

The **Web > Reporting > Web Sites** page is an overall aggregation of the activity that is happening on the managed appliances. From this page you can monitor high-risk web sites accessed during a specific time range.

To access the **Web Sites** page, perform the following:

- 
- Step 1** On the Security Management appliance window, choose **Web > Reporting > Web Sites**.

The Web Sites page appears:

**Figure 5-4 Web Sites Page****Web Sites**

From the **Web Sites** page, you can view the following information:

**Table 5-5**      ***Details on the Web > Reporting > Web Sites Page***

| Section                           | Description                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Range (drop-down list)       | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| Top Domains by Total Transactions | This section lists the top domains that are being visited on the site in a graph format.                                                                                                                                                        |



**Table 5-5**      *Details on the Web > Reporting > Web Sites Page*

| Section                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Top Domains by Transactions Blocked</b> | This section lists the top domains that triggered a block action to occur per transaction in a graph format. For example, a user went to a certain domain and because of a specific policy that I have in place, this triggered a block action. This domain then gets listed in this graph as a transaction blocked, and the domain site that triggered the block action is listed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Domains Matched</b>                     | <p>This section lists the domains that are that are being visited on the site in an interactive table. From this table you can access more granular information about a specific domain by clicking on the specific domain. The Web Tracking page appears and you can see tracking information and why certain domains were blocked.</p> <p>You can configure the columns that you want to appear in the Domains Matched section. For information on configuring columns for this section, see the <a href="#">“Interactive Report Pages for the Web Security Appliance”</a> section on page 5-10.</p> <p>After you have selected the Domains Matched categories to appear in the Domains Matched table, you can select how many items you want to be displayed from the Items Displayed drop-down menu. Choices are: 10, 20, 50, or 100</p> <p>When you click on a specific domain you can see the top users of that domain, the top transactions on that domain, the URL Categories matched and the Malware threats that have been detected. This table can be modified using the Time Range drop-down list so you can see a specific time range, such as hour, day or week for that domain use.</p> <p>To view an example of how Web Tracking may be used, see <a href="#">“Example 2: Tracking a URL”</a> section on page D-7.</p> |

From the **Web Sites** page you can also print or export the Top Domains by Total Transaction and the Domains Matched to a CSV file. For information on printing or exporting a file, see the [“Printing Reports from Report Pages”](#) section on page 5-11.

**Note**

You can generate a scheduled report for information on the Web Sites page. For information on scheduling a report, see the [“Scheduling Reports” section on page 5-82](#).

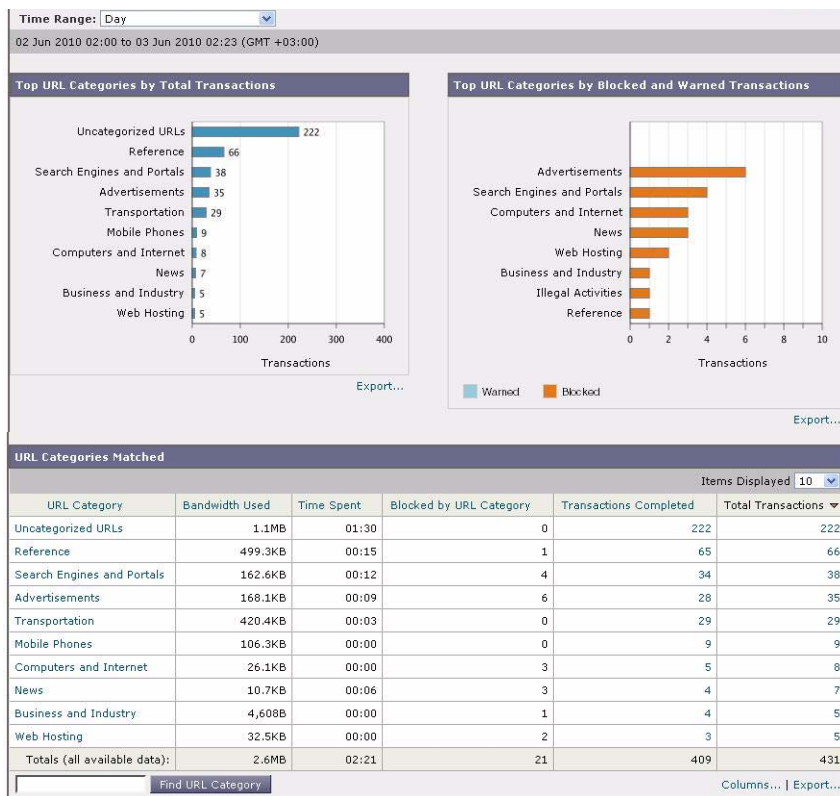
## URL Categories Page

The **Web > Reporting > URL Categories** page can be used to view the URL categories that are being visited by users on your system.

To access the **URL Categories** page, perform the following:

- 
- Step 1** On the Security Management appliance window, choose **Web > Reporting > URL Categories**.

The **URL Categories** page appears.

**Figure 5-5 URL Categories Page**

From the **URL Categories** page, you can view the following information:

**Table 5-6**      *Details on the Web > Reporting > URL Categories Page*

| Section                                  | Description                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Range (drop-down list)              | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| Top URL Categories by Total Transactions | This section lists the top URL Categories that are being visited on the site in a graph format.                                                                                                                                                 |

**Table 5-6**      *Details on the Web > Reporting > URL Categories Page*

| Section                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Top URL Categories by Blocked and Warned Transactions</b> | This section lists the top URL that triggered a block or warning action to occur per transaction in a graph format. For example, a user went to a certain URL and because of a specific policy that is in place, this triggered a block action or a warning. This URL then gets listed in this graph as a transaction blocked or warning.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>URL Categories Matched</b>                                | <p>The URL Categories Matched section shows all the URL categories during a specified time range for both completed, warned and blocked transactions. This is an interactive table with interactive column headings that you can use to sort data as you need. The Items Displayed menu changes the number of URL categories displayed in the list.</p> <p>You can configure the columns that you want to appear in the URL Categories section. For information on configuring columns for this section, see the <a href="#">“Interactive Report Pages for the Web Security Appliance”</a> section on page 5-10.</p> <p>After you have selected the specific items to appear in the URL Categories table, you can select how many items you want to be displayed from the Items Displayed drop-down menu. Choices are: 10, 20, 50, or 100.</p> <p>Additionally, you can find a specific URL Category within the URL Category section. In the text field at the bottom of the URL Category section, enter the specific URL Category name and click <b>Find URL Category</b>.</p> <p>The percentage of uncategorized URLs on the URL Categories page is typically around 15-20%. If the percentage of uncategorized URLs is higher than that, consider the following options:</p> <ul style="list-style-type: none"> <li>For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. For more information, see the <a href="#">“Custom URL Categories”</a> section on page 5-33.</li> </ul> |

From the URL Categories page you can also print or export the each of the sections on the page to a CSV file. For information on printing or exporting a file, see the [“Printing Reports from Report Pages” section on page 5-11](#).



#### Note

You can generate a scheduled report for information on the URL Categories page. For information on scheduling a report, see the [“Scheduling Reports” section on page 5-82](#). Additionally, you can generate a more detailed report for URL Categories; see the [“Top URL Categories—Extended” section on page 5-85](#) and [“Top Application Types—Extended” section on page 5-87](#).

If Data Availability is used within a scheduled report for URL Categories, and there are gaps in data for any of the appliances, the following message is displayed at the bottom of the page: “Some data in this time range was unavailable.” If there are no gaps present, nothing appears.

## Using The URL Categories Page in Conjunction with Other Reporting Pages

One of the advantages of the URL Categories page is that it can be used in conjunction with the [Application Visibility Page](#) and the [Users Page](#) to investigate a particular user, but also what types of applications or websites that a particular user is trying to access.

For example, from the [URL Categories Page](#) you can generate a high level report for Human Resources which details all the URL categories that are visited by the site. From the same page, you can gather further details in the URL Categories interactive table about the URL category ‘Streaming Media’. By clicking on the Streaming Media category link, you can view the specific URL Categories report page. This page not only displays the top users that are visiting streaming media sites (in the Top Users by Category for Total Transactions section), but also displays the domains that are visited (in the Domains Matched interactive table) such as YouTube.com or QuickPlay.com.

At this point, you are getting more and more granular information for a particular user. Now, let’s say this particular user stands out because of their usage, and you want to find out exactly what they are accessing. From here you can click on the user in the Users interactive table. This action takes you to the [User Details Page](#), where you can view the user trends for that user, and find out exactly what they have been doing on the web.

If you wanted to go further, you can now get down to web tracking details by clicking on Transactions Completed link in the interactive table. This brings up the [Web Tracking Page](#) where you can see the actual details about what dates the user accessed the sites, the full URL, the time spent on that URL, etc.

To view another example of how the URL Categories page may be used, see [“Example 3: Investigating Top URL Categories Visited”](#) section on page D-8.

## Custom URL Categories

The Security Management appliance, just like the Web Security appliance, ships with many predefined URL categories by default, such as Web-based Reporting, and more. However, you can also create user defined custom URL categories that specify specific host names and IP addresses. You might want to create custom URL categories for internal sites or a group of external sites you know you can trust.



### Note

The Security Management appliance uses the first four characters of custom URL category names preceded by the letter “c\_” in the access logs. Consider the custom URL category name if you use Sawmill for Cisco IronPort to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill for Cisco IronPort cannot properly parse the access log entry. Instead, only use supported characters in the first four characters if you will use Sawmill for Cisco IronPort to parse the access logs. If you want to include the full name of a custom URL category in the access logs, add the %XF format specifier to the access logs.

It is possible to create multiple custom URL categories and include the same URL in each category. The order of the custom URL categories matters. Categories listed higher in the list take priority over categories listed lower. When you include these custom URL categories in the same Access, Decryption, or Cisco IronPort Data Security Policy group and define different actions to each category, the action of the higher included custom URL category takes effect.

To create, edit, or delete a custom URL category:

- Step 1** On the Security Management appliance window, choose **Web > Configuration Master 7.1 > Custom URL Categories**.

The Custom URL categories page appears.

To edit an existing custom URL category, click the name of the URL category. To delete the custom URL category, click on the trash can across from the custom URL category you want to delete.

**Figure 5-6 Custom URL Categories Page**

**Custom URL Categories**



- Step 2** To create or edit a custom URL category, click **Add Custom Category**. The **Create Custom URL Categories: Add Category** page appears.

**Figure 5-7 Creating a Custom URL Category**

**Custom URL Categories: Add Category**

- Step 3** Enter the following settings in the appropriate fields to create, or edit the custom URL category.
- **Category Name**—Enter a name for the URL category. This name appears when you configure URL filtering for policy groups.
  - **List Order**—Type the order in the list of custom URL categories to place this category in the text field. Type **1** for the highest level URL category. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
  - **Sites**—Enter one or more addresses that belong in the custom category.



You can enter multiple addresses separated by line breaks or commas. You can enter addresses using any of the following formats:

- IP address, such as 10.1.1.0
- CIDR address, such as 10.1.1.0/24
- Domain name, such as example.com
- Hostname, such as crm.example.com
- Partial hostname, such as .example.com

**Note**

Entering a partial hostname, such as .example.com, also matches www.example.com.

- **Advanced**—In the Regular Expressions text field, type You can use regular expressions to specify multiple web servers that match the pattern you enter.

**Note**

The URL filtering engine compares URLs with addresses entered in the Sites field first. If the URL of a transaction matches an entry in the Sites field, it is not compared to any expression entered here.

**Step 4** (Optional) Click **Sort URLs** to sort all addresses in the Sites field.

By clicking **Sort URLs**, the site URLs will be sorted in alpha-numerical order. The original order that you entered for the sites in the list order will not be retained once they are sorted.

**Step 5** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes on the appliance.

## Reporting Misclassified and Uncategorized URLs

You can report misclassified and uncategorized URLs to the Cisco IronPort support portal at the following URL:

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

These get picked up and get evaluated for subsequent rule updates.

Verify that Web Reputation Filtering and Anti-Malware Filtering is enabled.

Often times, the correlation between malware and URLs with suspect content is high and it is likely that they may get caught by subsequent filters. The system pipeline is set up to catch malicious traffic with other downstream filters if URL filtering does not have a verdict. For more information on this, see the *Cisco IronPort AsyncOS for Web User Guide*.

## Application Visibility Page



### Note

For detailed information on Application Visibility, see the ‘Understanding Application Visibility and Control’ chapter in the *Cisco IronPort AsyncOS for Web User Guide*.

The **Web > Reporting > Application Visibility** page allows you to apply controls to particular application types within the Security Management appliance and Web Security appliance.

Not only does application control gives you more granular control over web traffic than just URL filtering, for example, it gives you more control over the following types of applications, and application types:

- Evasive applications, such as anonymizers and encrypted tunnels.
- Collaboration applications, such as Cisco WebEx, Facebook, and instant messaging.
- Resource intensive applications, such as streaming media.

## Understanding the Difference between Application versus Application Types

It is crucial to understand the difference between an application and an application types so that you can control the applications involved for your reports.

- **Application Types.** A category that contains one or more applications. For example, **search engines** is an application type that may contain search engines such as Google Search and Craigslist. Instant messaging is another application type category which may contain Yahoo Instant Messenger, or Cisco WebEx. Facebook is also an application type.

- **Applications.** Particular applications that belong in an application type. For example, YouTube is an application in the Media application type.
- **Application behaviors.** Particular actions or behaviors that users can accomplish within an application. For example, users can transfer files while using an application, such as Yahoo Messenger. Not all applications include application behaviors you can configure.

**Note**

For detailed information on understanding how you can use Application Visibility and Control (AVC) engine to control Facebook activity, see the ‘Understanding Application Visibility and Control’ chapter in the *Cisco IronPort AsyncOS for Web User Guide*.

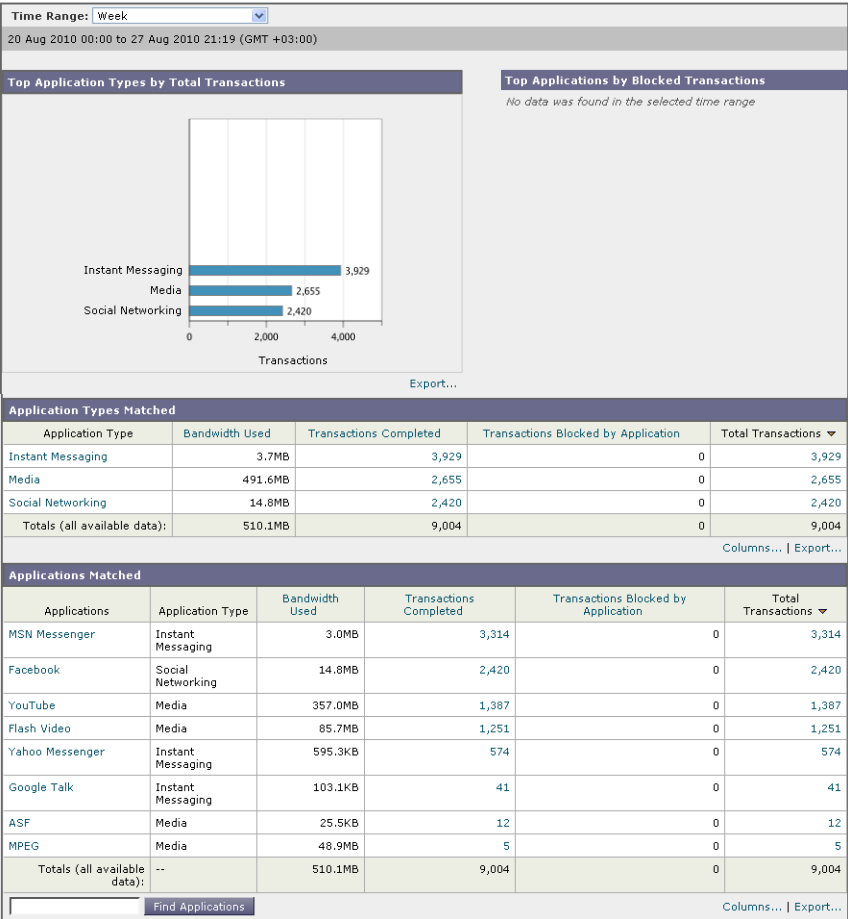
To access the **Application Visibility** page, perform the following:

- Step 1** On the Security Management appliance window, choose **Web > Reporting > Application Visibility**.

The **Application Visibility** page appears.

**Figure 5-8 Application Visibility Page**  
**Application Visibility**

Printable (PDF)



From the **Application Visibility** page, you can view the following information:

**Table 5-7**      ***Details on the Web > Reporting > Application Visibility Page***

| Section                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>                 | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                      |
| <b>Top Application Types by Total Transactions</b> | This section lists the top application types that are being visited on the site in a graph format. For example, instant messaging tools such as Yahoo Instant Messenger, Facebook, and Presentation application types.                                                                                                                                                                                               |
| <b>Top Applications by Blocked Transactions</b>    | This section lists the top application types that triggered a block action to occur per transaction in a graph format. For example, a user has tried to start a certain application type, for example Google Talk or Yahoo Instant Messenger, and because of a specific policy that is in place, this triggered a block action. This application then gets listed in this graph as a transaction blocked or warning. |

**Table 5-7**      *Details on the Web > Reporting > Application Visibility Page*

| Section                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Types Matched | The Application Types Matched interactive table allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions table. From the Applications column you can click on an application to view details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Applications Matched      | <p>The Applications Matched section shows all the application during a specified time range. This is an interactive table with interactive column headings that you can use to sort data as you need.</p> <p>You can configure the columns that you want to appear in the Applications Matched section. For information on configuring columns for this section, see the <a href="#">“Interactive Report Pages for the Web Security Appliance”</a> section on page 5-10.</p> <p>After you have selected the specific items to appear in the Applications table, you can select how many items you want to be displayed from the <b>Items Displayed</b> drop-down menu. Choices are: 10, 20, 50, or 100.</p> <p>Additionally, you can find a specific Application within the Application Matched section. In the text field at the bottom of this section, enter the specific Application name and click <b>Find Application</b>.</p> |



**Note**

You can generate a scheduled report for information on the Application Visibility page. For information on scheduling a report, see the [“Scheduling Reports”](#) section on page 5-82.

# Anti-Malware Page

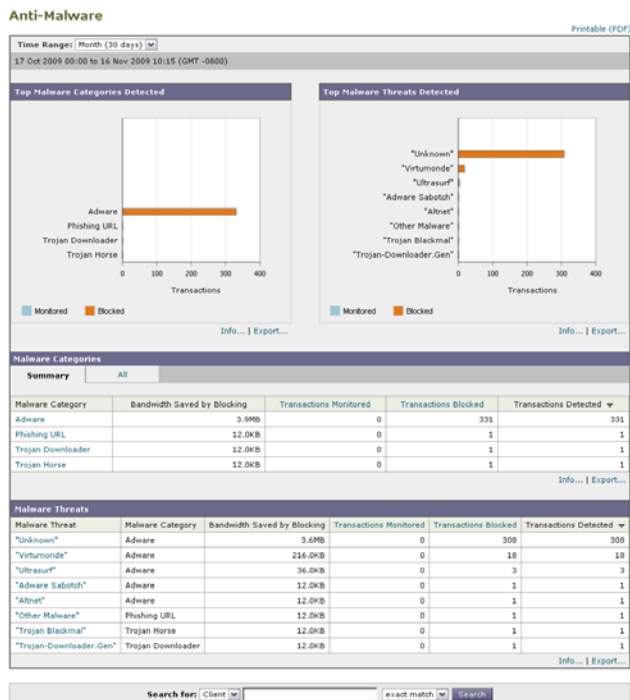
The **Web > Reporting > Anti-Malware** page is a security-related reporting page specifically based on the DVS engines such as WebRoot, Sophos, or McAfee. This page can be used to identify and stop a broad range of web-based malware threats and to monitor any malware detected.

To access the **Anti-Malware** page, perform the following step:

- Step 1** On the Security Management appliance window, choose **Web > Reporting > Anti-Malware**.

The Anti-Malware page appears:

**Figure 5-9 Anti-Malware Page**



From the **Anti-Malware** page, you can view the following information:

**Table 5-8**      *Details on the Web > Reporting > Anti-Malware Page*

| Section                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>     | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                                                                       |
| <b>Top Malware Categories Detected</b> | This section displays the top malware categories that are detected by a given category type with your chosen DVS engine. This information is displayed in graph format. See <a href="#">Table 5-9 on page 5-45</a> for more information on valid Malware categories.                                                                                                                                                                                                                  |
| <b>Top Malware Threats Detected</b>    | This section displays the top malware threats that are detected with your DVS engine. This information is displayed in graph format.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Malware Categories</b>              | <p>The Malware Categories interactive table shows detailed information about particular malware categories that are displayed in the Top Malware Categories Detected section.</p> <p>Clicking on any of the links in the Malware Categories interactive table allows you to view more granular details about individual malware categories and where they are on the network.</p> <p>See <a href="#">Table 5-9 on page 5-45</a> for more information on valid Malware categories.</p> |
| <b>Malware Threats</b>                 | The Malware Threats interactive table shows detailed information about particular malware threats that are displayed in the Top Malware Threats section.                                                                                                                                                                                                                                                                                                                              |

## Malware Category Report Page

The Malware Category Report page allows you to view detailed information on an individual Malware Category and what it is doing on your network.

To access the Malware Category report page, perform the following:

- Step 1**      On the Security Management appliance window, choose **Web > Reporting > Anti-Malware**.



The **Anti-Malware** page appears.

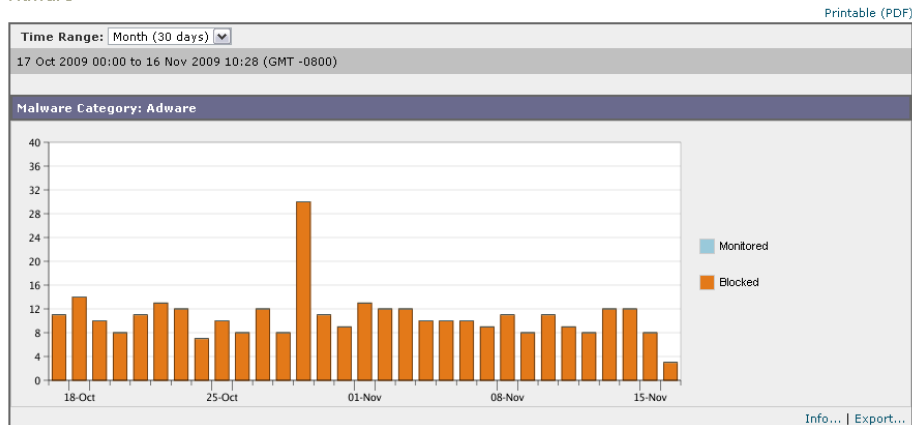
- Step 2** In the Malware Categories interactive table, click on a category in the Malware Category column.

The Malware Category report page appears.

**Figure 5-10 Malware Category Report Page**

#### Malware Category

Adware



## Malware Threat Report Page

The Malware Threat Report page report shows clients at risk for a particular threat, displays a list of potentially infected clients, and links to the Client Detail page. The trend graph at the top of the report shows monitored and blocked transactions for a threat during the specified time range. The table at the bottom shows the actual number of monitored and blocked transactions for a threat during the specified time range.

To access the Malware Threat report page, perform the following:

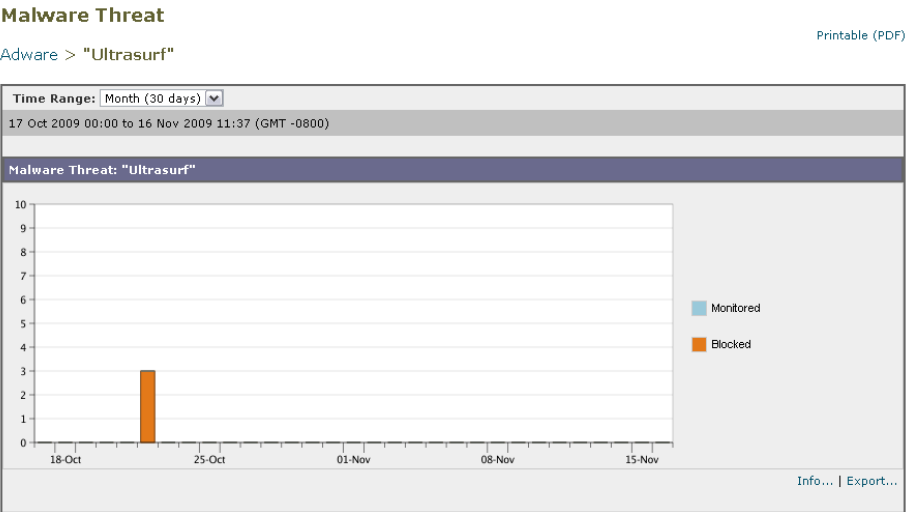
- Step 1** On the Security Management appliance window, choose **Web > Reporting > Anti-Malware**.

The Anti-Malware page appears.

**Step 2** In the Malware Threat interactive table, click on a category in the Malware Category column.

The Malware Threat report page appears:

**Figure 5-11 Malware Threats Report Page**



**Note**

You can generate a scheduled report for Top Malware Categories Detected and Top Malware Threats Detected on the Anti-Malware page, but you cannot schedule a generated report from the Malware Categories and Malware Threats Report Page. For information on scheduling a report, see the [“Scheduling Reports”](#) section on page 5-82.

## Malware Category Descriptions

Table 5-9 describes the different categories of malware the Security Management appliance and Web Security appliance can block

**Table 5-9** *Malware Category Descriptions*

| Malware Type                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Adware</b>                    | Adware encompasses all software executables and plug-ins that direct users towards products for sale. Some adware applications have separate processes that run concurrently and monitor each other, ensuring that the modifications are permanent. Some variants enable themselves to run each time the machine is started. These programs may also change security settings making it impossible for users to make changes to their browser search options, desktop, and other system settings. |
| <b>Browser Helper Object</b>     | A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Commercial System Monitor</b> | A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.                                                                                                                                                                                                                                                                                                                                        |
| <b>Dialer</b>                    | A dialer is a program that utilizes your modem or another type of Internet access to connect you to a phone line or a site that causes you to accrue long distance charges to which you did not provide your full, meaningful, and informed consent.                                                                                                                                                                                                                                              |
| <b>Hijacker</b>                  | A hijacker modifies system settings or any unwanted changes to a user's system that may direct them to a website or run a program without a user's full, meaningful, and informed consent.                                                                                                                                                                                                                                                                                                        |
| <b>Phishing URL</b>              | A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials.                                                                                                                                                                |
| <b>PUA</b>                       | Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.                                                                                                                                                                                                                                                                                                                                                                   |

**Table 5-9 Malware Category Descriptions (continued)**

| Malware Type      | Description                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Monitor    | A system monitor encompasses any software that performs one of the following actions:<br><br>Overtly or covertly records system processes and/or user action.<br><br>Makes those records available for retrieval and review at a later time.                                                                                                                                  |
| Trojan Downloader | A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host. These installations usually occur without the user’s knowledge. Additionally, a Trojan Downloader’s payload may differ from installation to installation since it obtains downloading instructions from the remote host/site. |
| Trojan Horse      | A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.                                                                                                                                                                                                                                  |
| Trojan Phisher    | A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passwords for bank sites, auction sites, or online payment sites.                                                                                                                                                  |
| Virus             | A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.                                                                                                                                                                                                                                                  |
| Worm              | A worm is program or algorithm that replicates itself over a computer network and usually performs malicious actions.                                                                                                                                                                                                                                                         |

# Configuring Anti-Malware



**Note**

Before you use the anti-malware feature on the Security Management appliance, you must first configure global settings on the Web Security appliance and then apply specific settings to different policies. For more information, see “Configuring Anti-Malware Scanning” in the *Cisco IronPort AsyncOS for Web User Guide*.

- To configure anti-malware, you must first configure the two following settings:
- **Global anti-malware settings.** Set object scanning parameters, specify global settings for URL matching, and control when to block the URL or allow processing to continue.

- **Access Policy anti-malware settings.** Enable monitoring or blocking for malware categories based on malware scanning verdicts.

**Step 1** On the Security Management appliance window, choose **Configuration Master 7.1 > Access Policies**.

The Access Policies window appears.

**Step 2** Click the link of the policy name in the Web Reputation and Anti-Malware Filtering column for the Access Policy you want to configure.

The **Access Policies: Reputation and Anti-Malware Settings** window for that policy appears.

On this page, you can enable monitoring or blocking for malware categories based on malware scanning verdicts.

**Step 3** In the Web Reputation and Anti-Malware Settings section, choose **Define Web Reputation and Anti-Malware Custom Settings** from the drop-down menu if it is not chosen already.

#### Web Access Policies: Reputation and Anti-Malware Settings: groupAuthPolicy



This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.

**Step 4** In the Cisco IronPort DVS Anti-Malware Settings section, configure the anti-malware settings for the policy as necessary.

Figure 5-12 Access Policy Anti-Malware Settings

IronPort DYS Anti-Malware Settings

☒ Enable Suspect User Agent Scanning ☒ Enable Webroot ☒ Sophos

|                                                                                            |            |
|--------------------------------------------------------------------------------------------|------------|
|                                                                                            | Monitor    |
| Malware Categories                                                                         | Select all |
| Adware                                                                                     | ✓          |
| Browser Helper Object                                                                      | ✓          |
| Commercial System Monitor                                                                  | ✓          |
| Dialer                                                                                     | ✓          |
| Hijacker                                                                                   | ✓          |
| Phishing URL                                                                               | ✓          |
| PUA                                                                                        | ✓          |
| System Monitor                                                                             | ✓          |
| Trojan Downloader                                                                          | ✓          |
| Trojan Horse                                                                               | ✓          |
| Trojan Phisher                                                                             | ✓          |
| Virus                                                                                      | ✓          |
| Worm                                                                                       | ✓          |
| Other Malware<br><i>(May include Worms, Trojans and other dangerous forms of malware.)</i> | ✓          |
|                                                                                            | Monitor    |
| Other Categories                                                                           | Select all |
| Encrypted File                                                                             | ✓          |
| Suspect User Agents                                                                        | ✓          |
| Unscannable                                                                                | ✓          |

**Step 5**     Configure the anti-malware settings for the policy as necessary.

Table 5-10 describes the anti-malware settings you can configure for Access Policies.

**Table 5-10**      ***Anti-Malware Settings for Access Policies***

| Setting                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Suspect User Agent Scanning</b> | Choose whether or not to enable the appliance to scan traffic based on the user agent field specified in the HTTP request header.<br><br>When you check this setting, you can choose to monitor or block suspect user agents in the Additional Scanning section at the bottom of the page.                                                                                                                                                                                                          |
| <b>Enable Webroot</b>                     | Choose whether or not to enable the appliance to use the Webroot scanning engine when scanning traffic. When you enable Webroot scanning, you can choose to monitor or block some additional categories in the Malware categories on this page.                                                                                                                                                                                                                                                     |
| <b>Enable Sophos</b>                      | Choose whether or not to enable the appliance to use the Sophos scanning engine when scanning traffic. When you enable Sophos scanning, you can choose to monitor or block some additional categories in the Malware categories on this page.                                                                                                                                                                                                                                                       |
| <b>Enable McAfee</b>                      | Choose whether or not to enable the appliance to use the McAfee scanning engine when scanning traffic. When you enable McAfee scanning, you can choose to monitor or block some additional categories in the Malware categories on this page.                                                                                                                                                                                                                                                       |
| <b>Malware Categories</b>                 | Choose whether to monitor or block the various malware categories based on a malware scanning verdict.<br><br>The categories listed in this section depend on which scanning engines you enable above.                                                                                                                                                                                                                                                                                              |
| <b>Additional Scanning</b>                | Choose whether to monitor or block the types of objects and responses listed in this section.<br><br><b>Note:</b> URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR, are considered unscannable transactions. |

- Step 6** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes on the appliance.
- 

For detailed information on Anti-Malware and how to configure this feature on the Web Security appliance, see “Configuring Anti-Malware Scanning” in the *Cisco IronPort AsyncOS for Web User Guide*.

## Client Malware Risk Page

The **Web > Reporting > Client Malware Risk** page is a security-related reporting page that can be used to monitor client malware risk activity.

From the Client Malware Risk page, a system administrator can see which of their users are encountering the most blocks or warnings. Given the information gathered from this page, the administrator can click on the user link to view what this user doing on the web that makes them run into so many blocks or warnings and setting off more detections than the rest of the users on the network.

Additionally, from the **Client Malware Risk** page you can see L4TM activity for a specific IP address.

To access the **Client Malware Risk** page, perform the following:

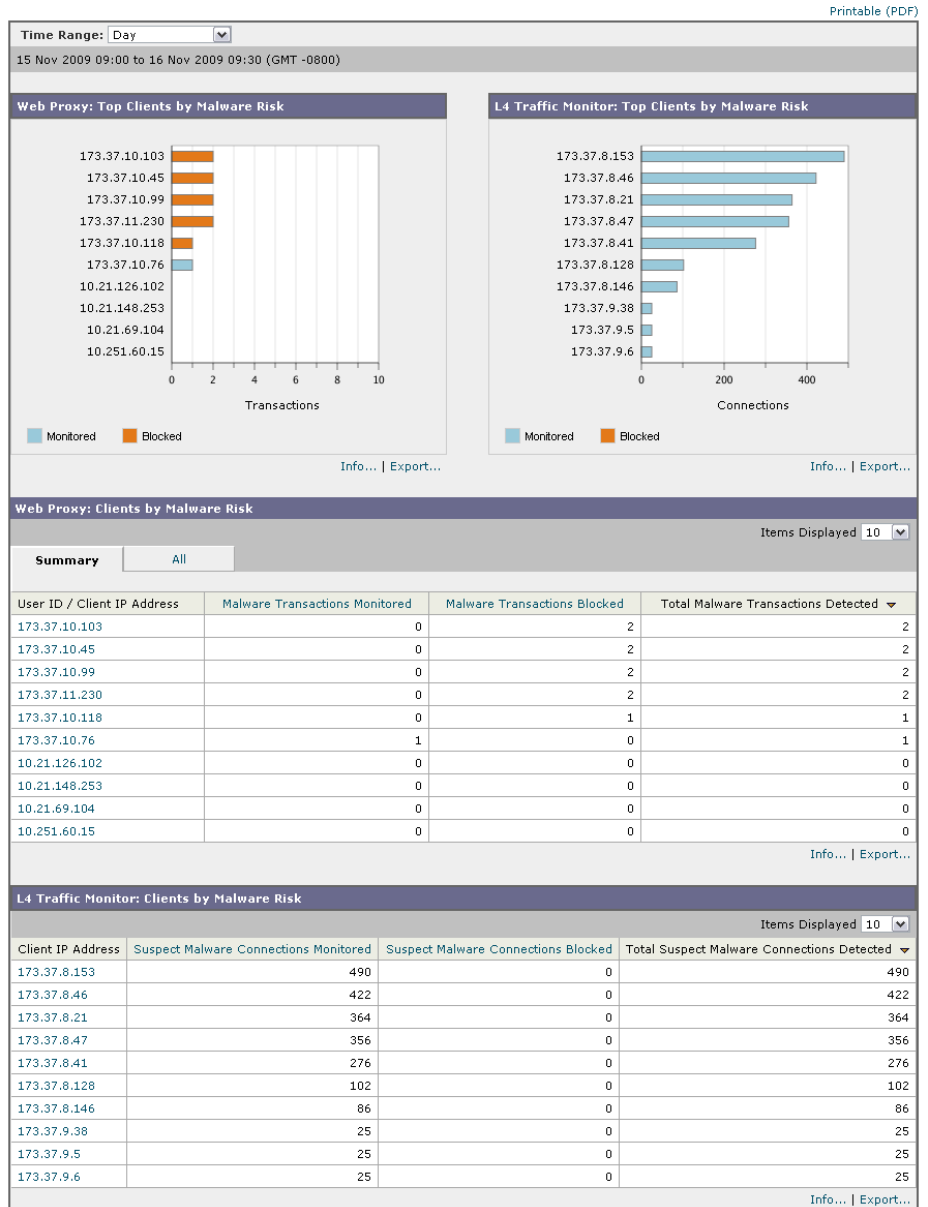
---

- Step 1** On the Security Management appliance window, choose **Web > Reporting > Client Malware Risk**.

The **Client Malware Risk** page appears.



**Figure 5-13 Client Malware Risk Page**  
**Client Malware Risk**



From the **Client Malware Risk** page, you can view the following information:

**Table 5-11**      *Details on the Web > Reporting > Client Malware Risk Page*

| Section                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>                     | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Web Proxy: Top Clients by Malware Risk</b>          | This section displays the top ten users that have encountered a malware risk. This information is displayed in graph format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>L4 Traffic Monitor: Top Clients by Malware Risk</b> | This section displays the top displays the top ten users that have encountered a L4 Traffic Monitoring risk. This information is displayed in graph format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Web Proxy: Clients by Malware Risk</b>              | <p>The Web Proxy: Clients by Malware Risk interactive table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section.</p> <p>The user ID’s and client IP addresses are interactive and link to a <a href="#">Client Detail Page</a> that provides detailed information respective to each client. See the <a href="#">Client Detail Page</a> section for more details on the Client Page.</p> <p>Clicking on any of the links in the interactive table allows you to view more granular details about individual users and what activity they are performing that is triggering the malware risk. For example, clicking on the link in the User/IP address column will take you to a User page for that IP address.</p> |
| <b>L4 Traffic Monitor: Clients by Malware Risk</b>     | The Web Proxy: Clients Malware Risk interactive table shows detailed information about individual users and what activity they are performing that is triggering the L4 Traffic Monitoring malware risk. Clicking on the link in the User/IP address column will take you to a User page for that IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



**Note**

You can generate a scheduled report for information on the Anti-Malware page. For information on scheduling a report, see the [“Scheduling Reports”](#) section on page 5-82.

## Client Detail Page

Clicking on the hypertext link of an individual client in the Web Proxy: Clients by Malware Risk section brings up the specific user's page that shows all the web activity and malware risk data for a particular client during the specified time range.

To access the Client Details page, perform the following:

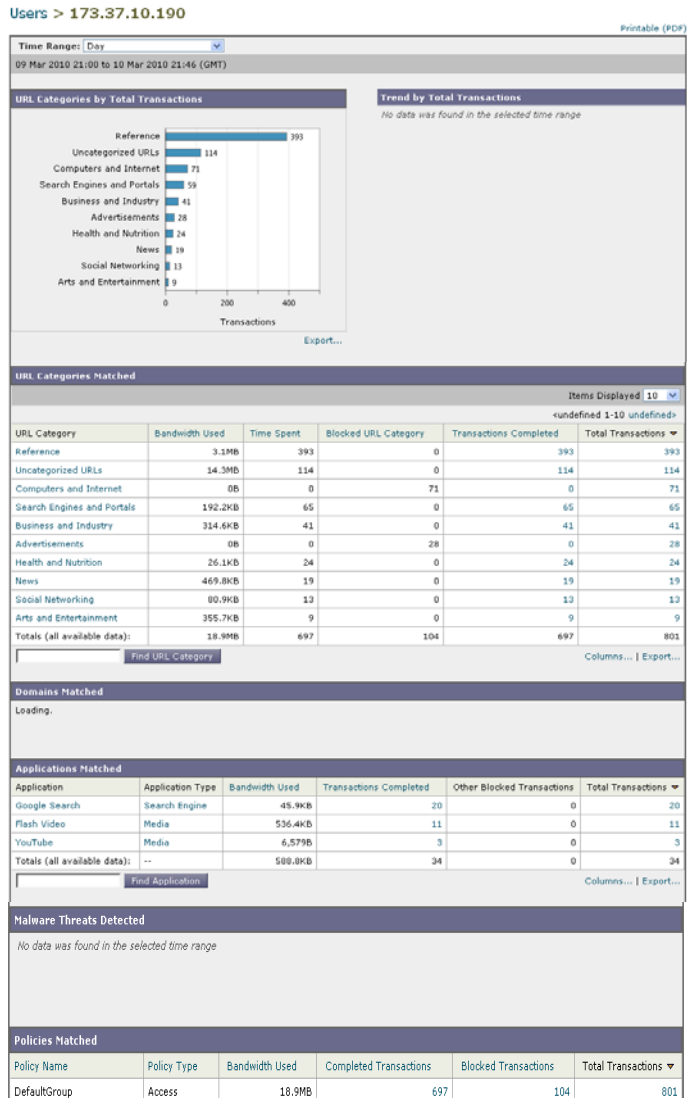
---

**Step 1** On the Security Management appliance window, choose **Web > Reporting > Client Malware Risk**.

The **Client Malware Risk** page appears.

**Step 2** Click on a link in the User/IP address column.

The Client Details page appears.

**Figure 5-14 Client Details Page**

From the **Client Details** page, you can view the following information:

**Table 5-12**      ***Details on the Web > Reporting > Client Malware Risk > Client Details Page***

| Section                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>          | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>URL Categories by Total Transactions</b> | This section lists the specific URL Categories that a specific user is using.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Trend by Total Transaction</b>           | <p>This graph indicates the trend of a specific users web transactions over time. In essence, when was this specific user on the web and at what times were they out browsing traffic.</p> <p>For example, this graph will indicate if there is a large spike in web traffic during certain hours of the day, and when those spikes occur. Using the Time Range drop-down list, you can expand this graph to see a more or less granular span of time that this user was on the web.</p>                                                                                                                                                                                                 |
| <b>URL Categories Matched</b>               | <p>The URL Categories Matched section shows all matched categories that could potentially be a Malware risk during a specified time range for both completed and blocked transactions. You can use interactive column headings to sort data, and the Items Displayed menu changes the number of URL categories displayed in the list.</p> <p>From this section you can also find a specific URL Category. In the text field at the bottom of the section enter the URL Category and click <b>Find URL Category</b>. The category does not need to be an exact match.</p> <p>Form more information on URL Categories, see <a href="#">“URL Categories Page”</a> section on page 5-28.</p> |

**Table 5-12**      *Details on the Web > Reporting > Client Malware Risk > Client Details Page*

| Section                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domains Matched</b>          | <p>From the Domains Matched section you can find out about a specific Domain or IP address that this user has accessed that could potentially be a Malware risk. You can also see the time spent on those categories, and various other information that you have set from the column view. In the text field at the bottom of the section enter the Domain or IP address and click <b>Find Domain or IP</b>. The domain or IP address does not need to be an exact match.</p>                                                                                                                                                                                          |
| <b>Applications Matched</b>     | <p>From this section you can find a specific application that a specific user is using that could potentially be a Malware risk.</p> <p>For example, if a user is accessing a site that requires use of a lot of Flash video, you will see the application type in the Application column. As a system administrator, you might have decided that anything with Flash video poses a Malware risk. Therefore, this application will show up in the Applications Matched section.</p> <p>In the text field at the bottom of the section enter the application name and click <b>Find Application</b>. The name of the application does not need to be an exact match.</p> |
| <b>Malware Threats Detected</b> | <p>From this table you can see the top Malware threats that a specific user is triggering that could potentially be a Malware risk. In the text field at the bottom of the Malware Threats section, enter the Malware Threat name and click <b>Find Malware Threat</b>. The name of the Malware Threat does not need to be an exact match.</p>                                                                                                                                                                                                                                                                                                                          |
| <b>Policies Matched</b>         | <p>From this section you can find a specific policy that is being enforced on this particular user that defines a certain action as a potential Malware risk.</p> <p>In the text field at the bottom of the section enter the policy name and click <b>Find Policy</b>. The name of the policy does not need to be an exact match.</p>                                                                                                                                                                                                                                                                                                                                  |

As with all of the web reporting pages, all of the tables in the **Client Details** page have interactive links to other details, as well as interactive column headings that can be configured to sort the data in each column specific to your needs for

viewing data on that page. For more information on configuring column settings, see the [“Interactive Report Pages for the Web Security Appliance”](#) section on page 5-10.

**Note**

The client reports sometimes show a user with an asterisk (\*) at the end of the user name. For example, the Client report might show an entry for both “jsmith” and “jsmith\*”. User names listed with an asterisk (\*) indicate the user name provided by the user, but not confirmed by the authentication server. This happens when the authentication server was not available at the time and the appliance is configured to permit traffic when authentication service is unavailable.

## Web Reputation Filters Page

The **Web > Reporting > Web Reputation Filters** is a security-related reporting page that allows you to view the results of your set Web Reputation filters for transactions during a specified time range.

### What are Web Reputation Filters?

Web Reputation Filters analyze web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. It helps protect against URL-based malware that threatens end-user privacy and sensitive corporate information. The Web Security appliance uses URL reputation scores to identify suspicious activity and stop malware attacks before they occur. You can use Web Reputation Filters with both Access and Decryption Policies.

Web Reputation Filters use statistically significant data to assess the reliability of Internet domains and score the reputation of URLs. Data such as how long a specific domain has been registered, or where a web site is hosted, or whether a web server is using a dynamic IP address is used to judge the trustworthiness of a given URL.

The web reputation calculation associates a URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a Web Reputation Score between -10 and +10, with +10 being the least likely to contain malware.

Example parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on any block lists
- Presence on any allow lists
- URL typos of popular domains
- Domain registrar information
- IP address information

For more information on Web Reputation Filtering, see ‘Web Reputation Filters’ in *Cisco IronPort AsyncOS for Web User Guide*.

To access the **Web Reputation Filters** page, perform the following:

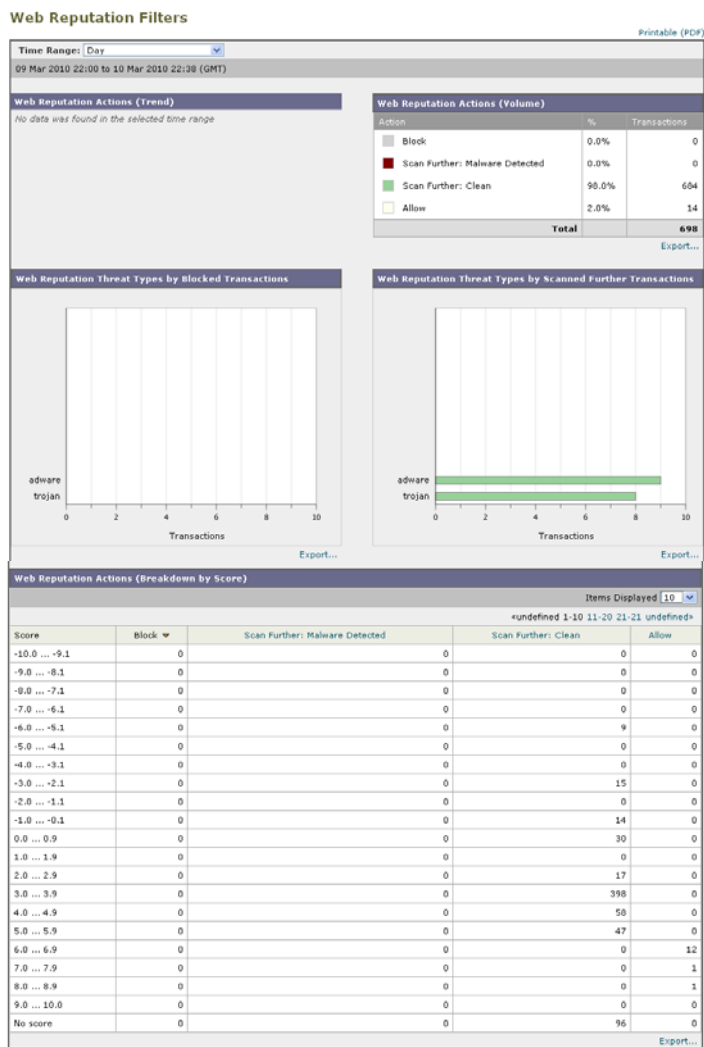
---

**Step 1** On the Security Management appliance window, choose **Web > Reporting > Web Reputation Filters**.

The **Web Reputation Filters** page appears.



Figure 5-15 Web Reputation Filter Page



From the **Web Reputation Filters** page, you can view the following information:

**Table 5-13**      ***Details on the Web > Reporting > Web Reputation Filters Page***

| Section                                                            | Description                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b>                                 | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.                             |
| <b>Web Reputation Actions (Trend)</b>                              | This section, in graph format, displays the total number of web reputation actions (vertical) against the time specified (horizontal timeline). From this you can see potential trends over time for web reputation actions.                                                |
| <b>Web Reputation Actions (Volume)</b>                             | This section displays the web reputation action volume in percentages by transactions.                                                                                                                                                                                      |
| <b>Web Reputation Threat Types by Blocked Transactions</b>         | This section displays the Web Reputation type that has been blocked.                                                                                                                                                                                                        |
| <b>Web Reputation Threat Types by Scanned Further Transactions</b> | This section displays the Web Reputation type that has been blocked and due to this action, needs to be scanned further.<br><br>If the result of Web Reputation filtering is to ‘Scan Further’, the transaction is passed to the Anti-Malware tool for additional scanning. |
| <b>Web Reputation Actions (Breakdown by Score)</b>                 | This interactive table displays the Web Reputation scores broken down for each action.                                                                                                                                                                                      |

The first four sections listed above contains the **Export** hypertext link to export data to a printable file. For information on printable files, see the [“Printing Reports from Report Pages”](#) section on page 5-11.

Additionally, the Web Reputation Actions table has interactive columns that can be configured. For more information on configuring interactive columns, see [“Configuring Column Settings on Report Pages”](#) section on page 5-10 and [“Interactive Columns for the Centralized Web Reporting Pages”](#) section on page E-1.

## Configuring Web Reputation Scores

When you install and set up the Security Management appliance and the Web Security appliance, the Web Security appliance has default settings for Web Reputation Scores. However, you can modify these threshold settings for web reputation scoring to fit your needs.

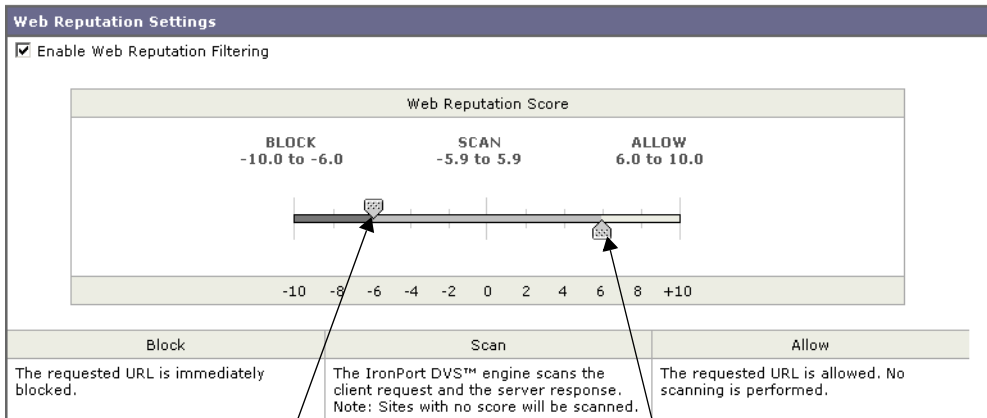
You must configure the web reputation filter settings for access policy and decryption policy groups.

### Configuring Web Reputation Filter Settings for Access Policies

To edit the web reputation filter settings for an Access Policy group:

- 
- Step 1** On the Security Management appliance window, choose **Configuration Master 7.1 > Access Policies**.
  - Step 2** Click the link under the Web Reputation and Anti-Malware Filtering column for the Access Policy group you want to edit.
  - Step 3** Under the Web Reputation and Anti-Malware Settings section, check the **Enable Web Reputation Filters** checkbox if it is not selected already.

The Web Reputation Score box becomes visible.

**Figure 5-16 Web Reputation Filter Settings for Access Policies**

Move these markers to change the Web Reputation threshold values

This allows you to override the web reputation and anti-malware settings from the Global Policy Group.

- Step 4** Verify the Enable Web Reputation Filtering field is enabled.
- Step 5** Move the markers to change the range for URL block, scan, and allow actions.
- Step 6** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes on the appliance.

At this point, you must configure Web Reputation for Decryption Policies. For information on editing or configuring the web reputation filter settings for a Decryption Policy group, see 'Web Reputation Filters' in *Cisco IronPort AsyncOS for Web User Guide*.

## L4 Traffic Monitor Data Page

The **Web > Reporting > L4 Traffic Monitor** page is a security-related reporting page that displays information about malware ports and malware sites that the L4 Traffic Monitor has detected during the specified time range.

The L4 Traffic Monitor listens to network traffic that comes in over all ports on the appliance and matches domain names, and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

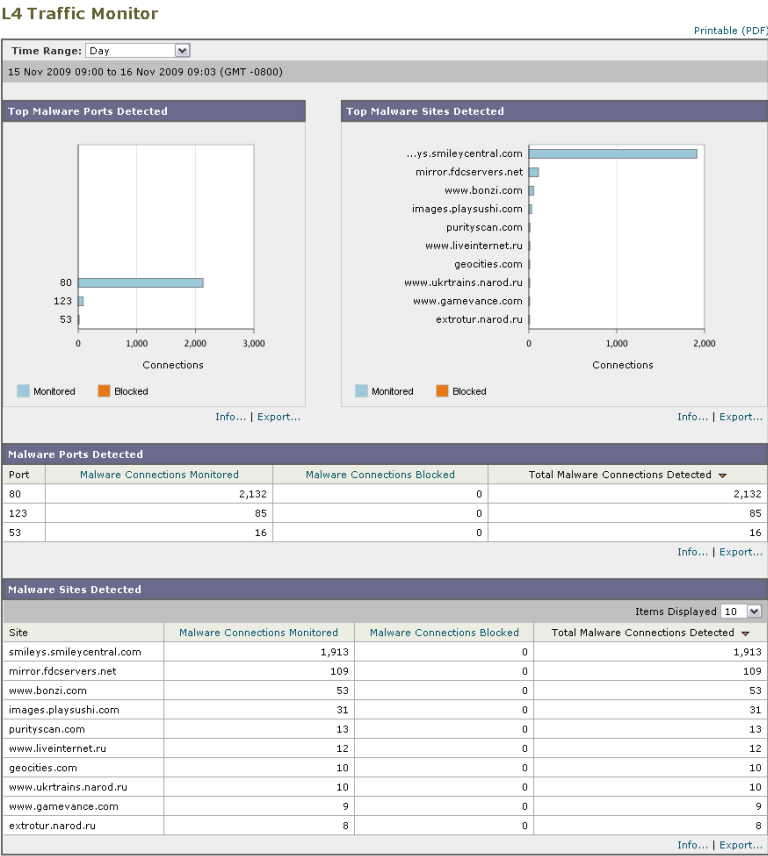
The upper part of the report displays the number of connections for each of the top malware ports and web sites. The lower part of the report displays malware ports and sites detected.

To access the **L4 Traffic Monitor Data** page, perform the following:

- 
- Step 1** On the Security Management appliance window, choose **Web > Reporting > L4 Traffic Monitor**.

The **L4 Traffic Monitor** page appears.

Figure 5-17 L4 Traffic Monitor Page



From the **L4 Traffic Monitor** page, you can view the following information:

**Table 5-14**      *Details on the Web > Reporting > L4 Traffic Monitor Page*

| Section                            | Description                                                                                                                                                                                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Range (drop-down list)</b> | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18.    |
| <b>Top Malware Ports Detected</b>  | This section displays, in graph format, the top Malware ports that have been detected by the L4 Traffic Monitor.                                                                                                                                   |
| <b>Top Malware Sites Detected</b>  | This section displays, in graph format, the top Malware domains that have been detected by the L4 Traffic Monitor.<br><br>In this view, the colored graph displays monitored or blocked domains that have been detected by the L4 Traffic Monitor. |
| <b>Malware Ports Detected</b>      | The Malware Ports Detected is a table that displays all of the ports that have been detected by the L4 Traffic Monitor.                                                                                                                            |
| <b>Malware Sites Detected</b>      | The Malware Sites Detected is a table that displays all of the domains that have been detected by the L4 Traffic Monitor.                                                                                                                          |

The sections listed above all contain the **Export** hypertext link to export data to a printable file. For information on printable files, see the [“Printing Reports from Report Pages”](#) section on page 5-11.

## Configuring the L4 Traffic Monitor

The L4 Traffic Monitor can be enabled as part of an initial system setup on the Security Management appliance by using the System Setup Wizard; choose **Management Appliance > System Administration > System Setup Wizard**.

By default, the L4 Traffic Monitor is enabled and set to monitor traffic on all ports. This includes DNS and other services.

To monitor true client IP addresses, the L4 Traffic Monitor should always be configured inside the firewall and before network address translation (NAT).

For information on configuring L4 Traffic Monitor settings, see the *Cisco IronPort AsyncOS for Web User Guide*. For more information on the System Setup Wizard, see the [“Understanding the System Setup Wizard”](#) section on page 2-9.

**Note**

You can generate a scheduled report for information on the L4 Traffic Monitor page. For information on scheduling a report, see the [“Scheduling Reports” section on page 5-82](#).

## Reports by User Location Page

The **Web > Reporting > Reports by User Location** Page allows you to find out what activities that your mobile users are conducting from their local or remote systems.

Activities include:

- URL Categories that are being accessed by the local and remote users.
- Anti-Malware activity that is being triggered by sites the local and remote users are accessing.
- Web Reputation of the sites being accessed by the local and remote users.
- Applications that are being accessed by the local and remote users.
- Users (local and remote).
- Domains accessed by local and remote users.

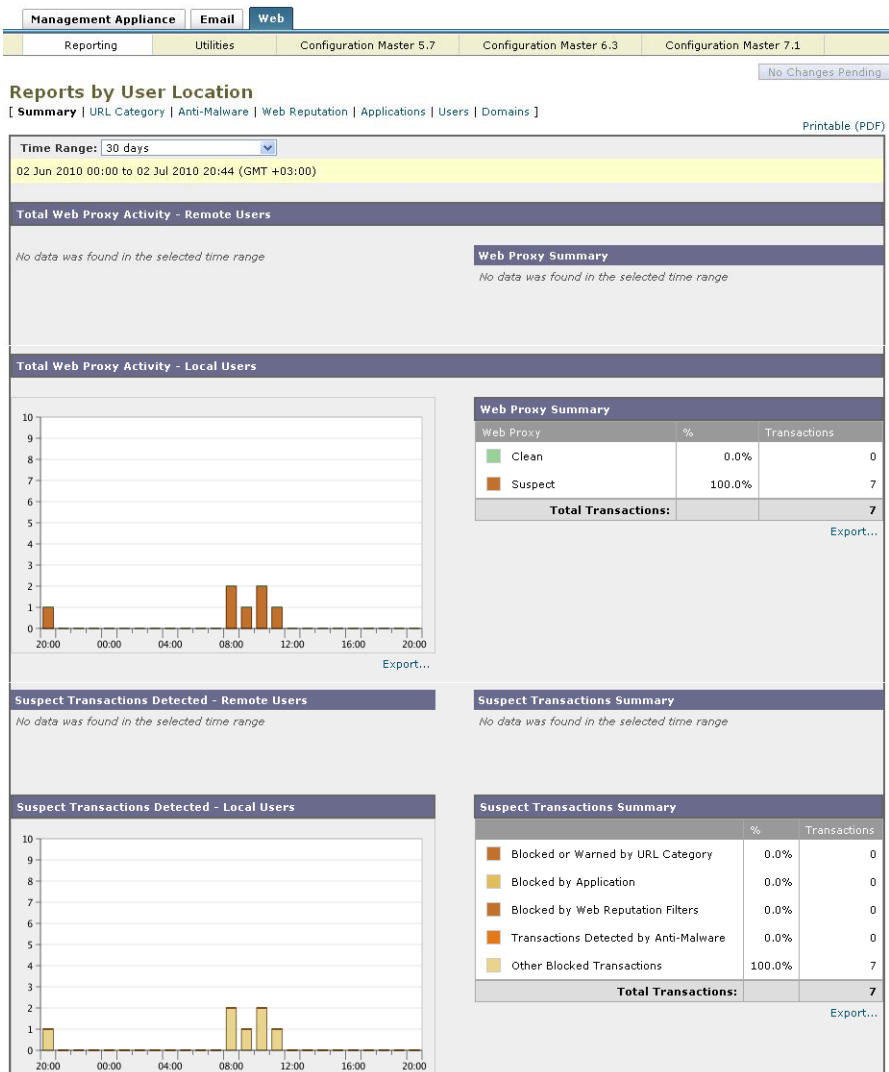
To access the **Reports by User Location** page, perform the following:

**Step 1** On the Security Management appliance window, choose **Web > Reporting > Reports by User Location**.

The **Reports by User Location** page appears.



Figure 5-18 Reports by User Location Page



From the **Reports by User Location** page, you can view the following information:

**Table 5-15**      *Details on the Web > Reporting > Reports by User Location Page*

| Section                                     | Description                                                                                                                                                                                                                                     |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Range (drop-down list)                 | A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the <a href="#">“Choosing a Time Range for Interactive Reports”</a> section on page 3-18. |
| Total Web Proxy Activity: Remote Users      | This section displays, in graph format, the activity of your remote users (vertical) over the specified time (horizontal).                                                                                                                      |
| Web Proxy Summary                           | This section displays a summary of the activities of the local and remote users on your system.                                                                                                                                                 |
| Total Web Proxy Activity: Local Users       | This section displays, in graph format, the activity of your remote users (vertical) over the specified time (horizontal).                                                                                                                      |
| Suspect Transactions Detected: Remote Users | This section displays, in graph format, the suspect transactions that have been detected due to access policies that you have defined for your remote users (vertical) over the specified time (horizontal).                                    |
| Suspect Transactions Summary                | This section displays a summary of suspected transactions of the remote users on your system.                                                                                                                                                   |
| Suspect Transactions Detected: Local Users  | This section displays, in graph format, the suspect transactions that have been detected due to access policies that you have defined for your remote users (vertical) over the specified time (horizontal).                                    |
| Suspect Transactions Summary                | This section displays a summary of suspected transactions of the local users on your system.                                                                                                                                                    |

From the **Reports by User Location** page you can generate reports showing the activity of local and remote users. This allows you to easily compare local and remote activities of your users.



**Note**

You can generate a scheduled report for information on the Reports by User Location page. For information on scheduling a report, see the [“Scheduling Reports”](#) section on page 5-82.

# Web Tracking Page

You can use the **Web > Reporting > Web Tracking** page to track and see basic web-related information such as the type of web traffic that is being handled by the Web Security appliances. This includes information such as time ranges, and UserID and Client IP addresses, but also includes information like certain types of URLs, how much bandwidth that each connection is taking up, or tracking a specific user's web usage.

Filtering Malware information is also an important part of web tracking as well as tracking web sites by WBRS score ranges, or reputation threat. All of these criteria can now be searched and monitored using web tracking page. While there is no way to exclude data from your web tracking results, once you decide what criteria you want to track, you can add more and more to narrow down the result set.

The Web Tracking page is designed to give the administrator simple information about a user using the either the [Default Web Tracking Results](#) view, or more advanced information using the [Advanced Web Tracking Results](#) view.

For an example of how the Web Tracking page can be used with other web reporting pages, see the [“Using The URL Categories Page in Conjunction with Other Reporting Pages”](#) section on page 5-32.

**Note**

It is important to remember that web reporting allows you to retrieve all the domain information that a user goes to, not necessarily the specific URL that is accessed. For information on a specific URL that the user is accessing, what time they went to that URL, whether that URL is allowed, etc., use the Web Tracking page.

To access the **Web Tracking** page, perform the following:

- Step 1** On the Security Management appliance window, choose **Web > Reporting > Web Tracking**.
- The **Web Tracking** page appears.

**Figure 5-19 Web Tracking Page**

**Web Tracking**

| Search                                                                                        |                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Available: 22 Sep 2010 12:00 to 22 Sep 2010 17:59 (GMT +03:00)                                |                                                                                                                                                                                                                                                           |
| Time Range:                                                                                   | 90 days                                                                                                                                                                                                                                                   |
| User/Client IP:                                                                               | (e.g. jdoe or DOMAIN\jdoe)                                                                                                                                                                                                                                |
| Website:                                                                                      | (e.g. google.com)                                                                                                                                                                                                                                         |
| Transaction Type:                                                                             | All Transactions                                                                                                                                                                                                                                          |
| <input checked="" type="radio"/> Advanced <i>Search transactions using advanced criteria.</i> |                                                                                                                                                                                                                                                           |
| URL Category:                                                                                 | <input type="radio"/> Disable Filter<br><input checked="" type="radio"/> Filter by URL Category: Select Category...                                                                                                                                       |
| Application:                                                                                  | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by Application: (ex. Yahoo Instant Messenger)<br><input type="radio"/> Filter by Application Type: (ex. Instant Messenger)                                                |
| Policy:                                                                                       | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by Policy:                                                                                                                                                                |
| Malware Threat:                                                                               | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by Malware Threat: (ex. W32/MyDoom-A)<br><input type="radio"/> Filter by Malware Category: Select Category...                                                             |
| WBRs:                                                                                         | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Score Range: -10 to 10<br><input type="radio"/> No Score<br><input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by Reputation Threat: (ex. phishing) |
| Mobile User Security:                                                                         | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by User Location: Remote access                                                                                                                                           |
| Web Appliance:                                                                                | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by Web Appliance: Select Appliance...                                                                                                                                     |
| User Request:                                                                                 | <input checked="" type="radio"/> Disable Filter<br><input type="radio"/> Filter by User-Requested Transactions                                                                                                                                            |
| <input type="button" value="Clear"/> <input type="button" value="Search"/>                    |                                                                                                                                                                                                                                                           |



**Note**

The Web Tracking Page is displayed above with the Advanced fields showing.

The Web Tracking page includes the following information:

**Default Web Tracking Results**

- Time Range
- User/Client IP
- Website

- Transaction Type

### Advanced Criteria Web Tracking Results

- URL Category
- Application
- Policy
- Malware Threat
- Web-based Reporting System (WBRs)
- Mobile User Security
- Web Appliance
- User Request

## Configuring Web Tracking

You can display the results of your web tracking with two possible views:

- [Default Web Tracking Results](#)
- [Advanced Web Tracking Results](#)

### Default Web Tracking Results

The Default Web Tracking view allows you to filter your web tracking results with basic criteria such as filtering by user name or IP address, transaction types, and so forth.

To gather Default Web Tracking results, perform the following steps:

- 
- Step 1** On the Security Management appliance, choose **Web > Reporting > Web Tracking**.

The Web Tracking page appears.

- Step 2** From the **Time Range** drop-down list, choose the time range that you want to track.

For information on time ranges and how they work on the Security Management appliance, see the [“Choosing a Time Range for Interactive Reports”](#) section on page 3-18.

- Step 3** Type in the User or Client IP address in the **User/Client IP** and **Website** fields. These are the Websites and User or Client IP addresses that you want tracking information for.
- Step 4** From the **Transaction Type** drop-down list, choose the types of transactions that you want to track.
- Choices include: All Transactions, Completed, Blocked, Monitored, and Warned.
- Step 5** Click **Search**.

The default view results are not configurable by column. Results are sorted by time stamp, with the most recent result at the top. The default view results look similar to the following page.

**Figure 5-20** *Default Web Tracking View Results Page*

| Results                        |                           |         |                    |                      |           |                    |
|--------------------------------|---------------------------|---------|--------------------|----------------------|-----------|--------------------|
| Displaying 1 - 46 of 46 items. |                           |         |                    |                      |           | Items Displayed 50 |
| Time (GMT +07:00)              | Website                   | (count) | Display Details... | Disposition          | Bandwidth | User / Client IP   |
| 10 Aug 2010 06:45:10           | http://fishki.net         |         |                    | Blocked by URL Cat   | 0B        | 10.251.60.45       |
| 10 Aug 2010 02:26:57           | http://engine.adland.ru   |         | (2)                | Blocked by Policy    | 0B        | 10.251.60.45       |
| 10 Aug 2010 02:26:54           | http://pic5.teasernet.com |         |                    | Blocked by WBRS -7.0 | 0B        | 10.251.60.45       |
| 10 Aug 2010 02:25:54           | http://engine.adland.ru   |         | (2)                | Blocked by Policy    | 0B        | 10.251.60.45       |
| 10 Aug 2010 02:25:52           | http://pic9.teasernet.com |         |                    | Blocked by Policy    | 0B        | 10.251.60.45       |
| 10 Aug 2010 02:25:02           | http://counter.yadro.ru   |         |                    | Blocked by WBRS -7.0 | 0B        | 10.251.60.45       |
| 10 Aug 2010 02:25:02           | http://is.luxup.ru        |         | (4)                | Blocked by WBRS -7.0 | 0B        | 10.251.60.45       |

In the Results window, you can view the following:

- The time the URL was accessed
- The Transaction website

Click on **Display Details** in the Transactions column to view more information about the transactions

- Disposition

The disposition column shows the reason that the transaction was blocked, whether blocked by policy, by WBRS score, and so forth.

- Bandwidth
- User ID/Client IP

## Advanced Web Tracking Results

The Advanced Web Tracking view allows you to filter your web tracking results with more advanced criteria such as filtering by WBRS reputation scores, by URL Categories, by Web Reputation threat and so forth.

To gather Advanced Web Tracking results, perform the following steps:

- 
- Step 1** On the Security Management appliance window, choose **Web > Reporting > Web Tracking**.
- The Web Tracking page appears.
- Step 2** From the **Time Range** drop-down list, choose the time range that you want to track.
- For information on time ranges and how they work on the Security Management appliance, see the [“Choosing a Time Range for Interactive Reports” section on page 3-18](#).
- Step 3** Type in the User or Client IP address in the **User/Client IP** and **Website** fields.
- These are the Websites and User or Client IP addresses that you want tracking information for.
- Step 4** From the **Transaction Type** drop-down list, choose the types of transactions that you want to track.
- Choices include: All, Completed, Blocked, Monitored, and Warned.
- Step 5** Click the **Advanced** arrow to expand the page to the Advanced Criteria view.
- Step 6** Click on the radio button next to **Filter by URL Category** to disable or enable a URL Category.
- Once you have enabled filtering by a URL Category, you can choose which category you want to enable by selecting from the choices in the **Filter By URL Category** drop-down list.
- Step 7** To filter by a specific policy, click on the radio button next to **Filter by Policy** and enter the policy name in the text field.
- Make sure that you have declared the policy on the Web Security appliance.
- Step 8** To filter by a specific Malware threat, click on the radio button next to **Filter by Malware Threat** and enter the threat name in the text field.

- Step 9** Click on the radio button next to Score Range to specify the score range of the WBRs.
- You can also disable this filter by clicking on the Disable Filter radio button in the WBRs section. For more information on WBRs score range information, see the *Cisco IronPort AsyncOS for Web User Guide*.
- Step 10** To filter web tracking by the reputation threat, click on the **Filter by Reputation Threat** radio button in the WBRs section. You can also disable this filter by clicking on the **Disable Filter** radio button in this section.
- Step 11** To filter by a specific Mobile User Security, click on the radio button next to **Filter by User Location** and enter the location in the text field. You can also disable this filter by clicking on the **Disable Filter** radio button in this section.
- Step 12** To filter by a specific Web appliance, click on the radio button next to **Filter by Web Appliance** and enter the Web appliance name in the text field. You can also disable this filter by clicking on the **Disable Filter** radio button in this section.
- Step 13** To filter by a specific User Request, click on the radio button next to **Filter by User-Requested Transaction** and enter the Web appliance name in the text field. You can also disable this filter by clicking on the **Disable Filter** radio button in this section.
- Step 14** To enable page view results, click on the checkbox next to **Enable Page** view Results.
- Step 15** Click **Search**.
- The results of your web tracking search appear.
- Step 16** Click on **Display Details** in the Transactions column to view more information about the transactions.
- 

For an example of Web Tracking usage, see [“Example 1: Investigating a User” section on page D-2](#).

## System Capacity Page

The **Web > Reporting > System Capacity** page allows you to view the overall workload that is put on the Security Management appliance by the Web Security appliances. Most importantly, you can use the System Capacity page to track



growth over time and plan for system capacity. Monitoring your Web Security appliances ensures that the capacity is appropriate to your volumes. Over time, volume inevitably rises and appropriate monitoring ensures that additional capacity or configuration changes can be applied proactively.

The System Capacity page can be used to determine the following information:

- Identify when Web Security appliances are exceeding recommended CPU capacity; this enables you to determine when configuration optimization or additional appliances are needed.
- For troubleshooting, identify which parts of the system are using the most resources.
- Identify response time and Proxy buffer memory.
- Identify the transactions per second, and any connections that are outstanding.

## How to Interpret the Data You See on System Capacity Page

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

- **Day Report**— The Day report queries the hour table and displays the exact number of queries that have been received by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table.
- **Month Report**— The Month report queries the day tables for the 30 or 31 days (dependent on the number of days in the month), giving you an exact report on the number of queries over 30 or 31 days. Again, this is an exact number.

The ‘Maximum’ value indicator on the System Capacity page is the highest value seen for the specified period. The ‘Average’ value is the average of all values for the specified period. The period of aggregation depends on the interval selected for that report. For example, you can choose to see the Average and Maximum values for each day if the chart is for a month period.



### Note

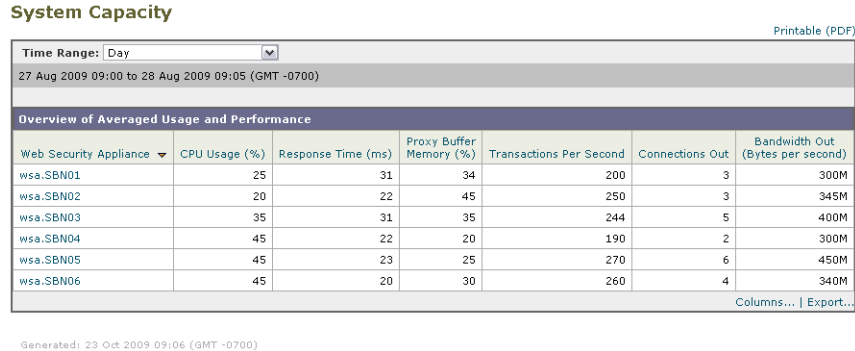
If you select **Year** for the time range to other reports, we recommend that you select the largest time range, 90 days.

To access the **System Capacity** page, perform the following:

**Step 1** On the Security Management appliance window, choose **Web > Reporting > System Capacity**.

The **System Capacity** page appears.

**Figure 5-21**      **System Capacity Page**



**Step 2** Click on a specific appliance in the Web Security appliance column on the Overview of Averaged Usage and Performance interactive table to see the system capacity for that appliance.

The System Capacity graphs appear for that user. The System Capacity Page has two type of information that you can view:

- [System Capacity—System Load](#)
- [System Capacity – Network Load](#)

## System Capacity—System Load

The first four graphs on the System Capacity window show the system load reports. These reports show the overall CPU usage on the appliances. AsyncOS is optimized to use idle CPU resources to improve transaction 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 processing for the Web Security appliance

reporting. The CPU-by-function graph is an 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.

Additionally, the Response Time/Latency and Transactions Per Second graphs shows the overall response time (in milliseconds), and transactions per second for the date range specified in the Time Range drop-down menu.

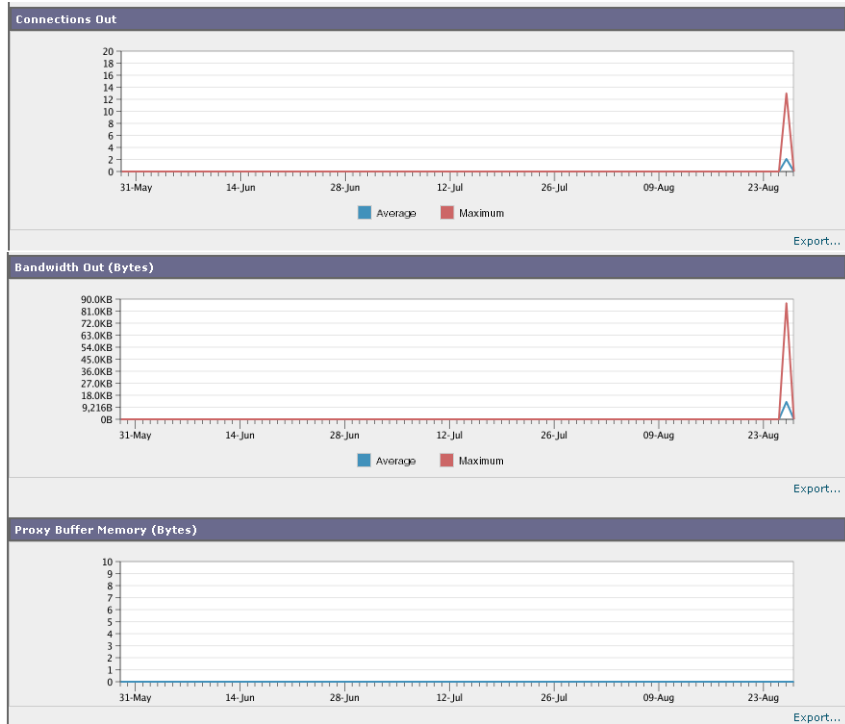
**Figure 5-22 System Capacity – System Load**

## System Capacity—Network Load

The next graphs on the System Capacity window show the outgoing connections, the bandwidth out, and the proxy buffer memory statistics. You can view the results for a day, week, month, or year. It is important to understand the trends of

normal volume and spikes in your environment.

**Figure 5-23 System Capacity – Network Load**



### Note About Proxy Buffer Memory Swapping

The system is designed to swap proxy buffer memory regularly, so some proxy buffer memory swapping is expected and is not an indication of problems with your appliance. Unless the system *consistently* swaps proxy buffer memory in high volumes, proxy buffer memory swapping is normal and expected behavior. If your system runs with extremely high volumes, and consistently swaps proxy buffer memory due to the high volumes, you may need to add Cisco IronPort appliances to your network or tune your configuration to ensure maximum throughput to improve performance.

You can configure the System Capacity column settings in the **Overview of Averaged Usage and Performance** section of the System Capacity page. For information on configuring interactive columns, see [“Configuring Column Settings on Report Pages” section on page 5-10](#) and [“Interactive Columns for the Centralized Web Reporting Pages” section on page E-1](#).

# Data Availability Page

The **Web > Reporting > Data Availability** page allows you to view, update and sort data to provide real-time visibility into resource utilization and web traffic trouble spots.

To access the **Data Availability** page, perform the following:

- Step 1
- On the Security Management appliance page, choose **Web > Reporting > Data Availability**.  
The **Web Reporting Data Availability** page appears.

**Figure 5-24**      **Web Reporting Data Availability Page**  
**Web Reporting Data Availability**

Printable (PDF)

| Web Reporting Data Range |                                |                                |                                   |                                |              |                           |
|--------------------------|--------------------------------|--------------------------------|-----------------------------------|--------------------------------|--------------|---------------------------|
| Web Security Appliance   | Web Reporting                  |                                | Web Tracking and Reporting Detail |                                | Missing Data | Status                    |
|                          | From                           | To                             | From                              | To                             |              |                           |
| wsa.SBN01                | 22 May 2009 10:20              | 06 Nov 2009 09:01              | 07 Aug 2009 10:01                 | 06 Nov 2009 09:01              | No           | OK                        |
| wsa.SBN02                | 22 May 2009 10:20              | 06 Nov 2009 08:48              | 07 Aug 2009 10:01                 | 06 Nov 2009 08:48              | No           | Not updated in 12 minutes |
| wsa.SBN03                | 22 May 2009 10:20              | 06 Nov 2009 08:57              | 07 Aug 2009 10:01                 | 06 Nov 2009 08:57              | No           | OK                        |
| wsa.SBN04                | 22 May 2009 10:20              | 06 Nov 2009 08:57              | 07 Aug 2009 10:01                 | 06 Nov 2009 08:57              | No           | OK                        |
| wsa.SBN05                | 22 May 2009 10:20              | 06 Nov 2009 08:57              | 07 Aug 2009 10:01                 | 06 Nov 2009 08:57              | Yes          | OK                        |
| wsa.SBN06                | 22 May 2009 10:20              | 06 Nov 2009 08:59              | 07 Aug 2009 10:01                 | 06 Nov 2009 08:59              | No           | OK                        |
| Overall:                 | 22 May 2009 10:20 (GMT -07:00) | 06 Nov 2009 09:01 (GMT -08:00) | 07 Nov 2009 10:20 (GMT -07:00)    | 07 Nov 2009 09:01 (GMT -08:00) |              |                           |

All data resource utilization and web traffic trouble spots are shown from this page.



**Note**

On the Web Reporting Data Availability page, web reporting will report as disabled only if both Web Reporting and Email Reporting are disabled on the individual Web and Email appliances. If Web Reporting is disabled, the Security Management appliance will not pull any new data from the Web Security

appliance, but previously retrieved data is still present on the Security Management appliance. For information on how to manage disk usage, see the [“Managing Disk Usage” section on page 12-115](#).

If the status is different between The Web Reporting ‘From’ and ‘To’ columns, and the Web Reporting and Tracking ‘From’ and ‘To’ columns, the most severe consequence appears in the Status column.

Additionally, if there is a gap in the overall ranges that have been configured in either web reporting or web tracking, **Yes** appears in the Missing Data column.

**Step 2** In the Web Security appliance column, click on the specific appliance that you want the data availability information from.

The Web Reporting Data Availability for that appliance appears. In this window you can view the following information:

- Data Received
- Date Range available for that specific appliance.  
This information is also reflected on the Overview page. In the Web Reporting section and the Web Tracking and Reporting Details section, the ‘From’ and ‘To’ headings are hyperlinks that allow you to view the specific web details for a specific user.

Data is only shown for intervals within a specific time period.

**Step 3** From the Items Displayed drop-down menu, you can choose how many records you want to display.

**Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes on the appliance.



**Note**

If Data Availability is used within a scheduled report for URL Categories, and there are gaps in data for any of the appliances, the following message is displayed at the bottom of the page: “Some data in this time range was unavailable.”  
If there are no gaps present, nothing appears.

# Scheduling Reports

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, previous month, previous calendar day (up to 250), previous calendar month (up to 12). Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months).

Regardless of when you run a report, the data is returned from the previous time interval (hour, day, week, or month). For example, if you schedule a daily report to run at 1AM, the report will contain data from the previous day, midnight to midnight (00:00 to 23:59).

You can schedule reports for the following types of reports:

- Web Reporting Overview—For information on what is included on this page, see the [“Web Reporting Overview Page” section on page 5-12](#).
- Users—For information on what is included on this page, see the [“Users Page” section on page 5-16](#).
- Web Sites—For information on what is included on this page, see the [“Web Sites Page” section on page 5-24](#).
- URL Categories—For information on what is included on this page, see the [“URL Categories Page” section on page 5-28](#).
- Top URL Categories — Extended: For information on how to generate a report for Top URL Categories — Extended, see the [Top URL Categories—Extended, page 5-85](#).
- Application Visibility—For information on what is included on this page, see the [“Application Visibility Page” section on page 5-36](#).
- Top Application Types — Extended: For information on how to generate a report for Top URL Categories — Extended, see the [Top Application Types—Extended, page 5-87](#).
- Anti-Malware—For information on what is included on this page, see the [“Anti-Malware Page” section on page 5-41](#).
- Client Malware Risk—For information on what is included on this page, see the [“Client Malware Risk Page” section on page 5-50](#).
- Web Reputation Filters—For information on what is included on this page, see the [“Web Reputation Filters Page” section on page 5-57](#).



- L4 Traffic Monitor—For information on what is included on this page, see the [“L4 Traffic Monitor Data Page” section on page 5-63](#).
- Mobile Secure Solution—For information on what is included on this page, see the [“Reports by User Location Page” section on page 5-66](#).
- System Capacity—For information on what is included on this page, see the [“System Capacity Page” section on page 5-74](#).

## Managing Scheduled Reports

This section includes the following:

- [Adding Scheduled Reports, page 5-83](#)
- [Editing Scheduled Reports, page 5-85](#)
- [Deleting Scheduled Reports, page 5-85](#)
- [Additional Extended Reports, page 5-85](#)



### Note

With any scheduled report, you can choose to make all user information unrecognizable. To generate reports so that user names are unrecognizable in reports, check the **Anonymize** usernames in reports checkbox. The default setting is that all usernames appear in all reports.

The Security Management appliance retains the most recent reports that 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, you may want to create a mailing list instead of listing the recipients individually.

By default, the appliance archives the twelve most recent reports of each scheduled report. Reports are stored in the **/periodic\_reports** directory of the appliance. (See [Appendix A, “Accessing the Appliance”](#) for more information.)

## Adding Scheduled Reports

To add a scheduled web report, use the following steps:

**Step 1** On the Security Management appliance window, choose **Web > Reporting > Scheduled Reports**.

**Step 2** Click **Add Scheduled Report**.

The Add Scheduled Report page appears.

**Figure 5-25 Add Scheduled Reports Page**

**Add Scheduled Report**

| Report Settings                     |                                                                                                                                                                                                 |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type:                               | Top URL Categories - Extended                                                                                                                                                                   |
| Title:                              | Top URL Categories - Extended                                                                                                                                                                   |
| Time Range To Include:              | Previous 7 calendar days                                                                                                                                                                        |
| Format:                             | <input checked="" type="radio"/> PDF <a href="#">Preview PDF Report</a>                                                                                                                         |
| Number of Items:                    | 5                                                                                                                                                                                               |
| Sort Column:                        | <div>Table</div> <div>Category[1]: Category Name <span>Transactions Total</span></div>                                                                                                          |
| Schedule:                           | <input type="radio"/> Daily At time: <span>01</span> : <span>00</span><br><input checked="" type="radio"/> Weekly on <span>Sunday</span><br><input type="radio"/> Monthly on first day of month |
| Email to:                           | <br><small>Separate multiple addresses with commas. Leave blank for archive only.</small>                                                                                                       |
| <div>Cancel</div> <div>Submit</div> |                                                                                                                                                                                                 |

**Step 3** From drop-down menu next to **Type**, choose your report type.

**Step 4** In the **Title** field, type the title of your report.

To avoid creating multiple reports with the same name, we recommend using a descriptive title.

**Step 5** Choose the time range for the report from the **Time Range** drop-down menu.

**Step 6** Choose the format for the generated report.

The default format is PDF. Most reports allow scheduling of CSV.

**Step 7** From the drop-down list next to **Number of Items**, choose the number of items that you want to be included in the generated report.

Valid values are from 2 through 20. The default value is 5.

**Step 8** From the drop-down list next to **Sort Column**, select the column to sort the data by for this report. This allows you to create a scheduled report of Top 'N' items by any column available in the scheduled report.

- Step 9** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.
- Step 10** In the **Email** text field, type in the email address where the generated report will be sent.
- If you do not specify an email address, the report is archived only.
- Step 11** Click **Submit**.
- 

## Editing Scheduled Reports

To edit reports, go to the **Web > Reporting > Scheduled Reports** page and select the check boxes corresponding to the reports that you want to edit. Modify settings then click **Submit** to submit your changes on the page, then click the **Commit Changes** button to commit your changes on the appliance.

## Deleting Scheduled Reports

To delete reports, go to the **Web > Reporting > Scheduled Reports** page and select the check boxes corresponding to the reports that you want to delete. To remove all scheduled reports, select the **All** check box, **Delete** and **Commit** your changes. Note that archived versions of deleted reports are not deleted.

## Additional Extended Reports

There are two additional extended reports that can be generated in the **Web > Reporting** section on the Security Management appliance. They are:

- [Top URL Categories—Extended](#)
- [Top Application Types—Extended](#)

### Top URL Categories—Extended

The Top URL Categories —Extended report is useful for administrators who want to receive more detailed information than the URL Categories report can provide.

For example, in a typical URL Categories report, you can gather information measuring bandwidth usage by a particular employee at a larger URL Category level. But, imagine that the network administrator wants to generate a more detailed report that monitors bandwidth usage for the top ten URLs for each URL Category, or top five users for each URL Category. At this stage, the administrator would use the Top URL Categories —Extended report.



**Note**

The maximum number of reports that can be generated using this type of report is 20.

To generate a Top URL Categories—Extended report, perform the following:

**Step 1** On the Security Management appliance window, choose **Web > Reporting > Scheduled Reports**.

**Step 2** Click **Add Scheduled Report**.

The Add Scheduled Report window appears.

**Add Scheduled Report**

| Report Settings                     |                                                                                                                                                                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type:                               | Top URL Categories - Extended                                                                                                                                                                                                                      |
| Title:                              | Top URL Categories - Extended                                                                                                                                                                                                                      |
| Time Range To Include:              | Previous 7 calendar days                                                                                                                                                                                                                           |
| Format:                             | PDF <a href="#">Preview PDF Report</a>                                                                                                                                                                                                             |
| Number of Items:                    | 5                                                                                                                                                                                                                                                  |
| Sort Column:                        | <div>Table</div> <div>Category[1]: Category Name</div> <div>Column</div> <div>Transactions Total</div>                                                                                                                                             |
| Schedule:                           | <div> <input type="radio"/> Daily           <input checked="" type="radio"/> Weekly           <input type="radio"/> Monthly         </div> <div>           on Sunday           <div>At time: 01 : 00</div> </div> <div>on first day of month</div> |
| Email to:                           | <div></div> <div><small>Separate multiple addresses with commas. Leave blank for archive only.</small></div>                                                                                                                                       |
| <div>Cancel</div> <div>Submit</div> |                                                                                                                                                                                                                                                    |

**Step 3** From drop-down menu next to Type, choose **Top URL categories — Extended**.

**Step 4** In the **Title** text field, type the title of your URL extended report.

**Step 5** Choose the time range for the report from the **Time Range** drop-down menu.

**Step 6** Choose the format for the generated report.

The default format is PDF.

- Step 7** From the drop-down list next to **Number of Items**, select the number of URL Categories that you want to be included in the generated report.
- Valid values are from 2 through 20. The default value is 5.
- Step 8** From the drop-down list next to Sort Column, select the column to sort the data by for this report. This allows you to create a scheduled report of Top 'N' items by any column available in the scheduled report.
- Step 9** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.
- Step 10** In the **Email** text field, type in the email address where the generated report will be sent.
- Step 11** Click **Submit**.
- 

## Top Application Types—Extended

To generate a Top Application Type—Extended report, perform the following:

- 
- Step 1** On the Security Management appliance window, choose **Web > Reporting > Scheduled Reports**.
- Step 2** Click **Add Scheduled Report**.
- The Add Scheduled Report window appears.

**Step 3** From drop-down menu next to Type, choose **Top Application Types — Extended**.

**Add Scheduled Report**

**Report Settings**

|                        |                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type:                  | Top Application Types - Extended                                                                                                                         |
| Title:                 | Top Application Types - Extended                                                                                                                         |
| Time Range To Include: | Previous 7 calendar days                                                                                                                                 |
| Format:                | <input checked="" type="radio"/> PDF <a href="#">Preview PDF Report</a><br><input type="radio"/> CSV                                                     |
| Number of Items:       | 5                                                                                                                                                        |
| Sort Column:           | Table Column<br>Type: Application Name Transactions Total                                                                                                |
| Schedule:              | <input type="radio"/> Daily At time: 01 : 00<br><input checked="" type="radio"/> Weekly on Sunday<br><input type="radio"/> Monthly on first day of month |
| Email to:              | <br><small>Separate multiple addresses with commas. Leave blank for archive only.</small>                                                                |

Cancel Submit

**Step 4** In the **Title** text field, type the title of your report.

**Step 5** Choose the time range for the report from the **Time Range** drop-down menu.

**Step 6** Choose the format for the generated report.

The default format is PDF.

**Step 7** From the drop-down list next to **Number of Items**, select the number of URL Categories that you want to be included in the generated report.

Valid values are from 2 through 20. The default value is 5.

**Step 8** From the drop-down list next to **Sort Column**, select the type of column that you want to appear in the table. Choices include: Transactions Completed, Transactions Blocked, Transaction Totals.

**Step 9** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

**Step 10** In the **Email** text field, type in the email address where the generated report will be sent.

**Step 11** Click **Submit**.

# Archiving Reports

The **Web > Reporting > Archived Reports** page lists available archived reports. Report names in the Report Title column are interactive and link to a view of each report. The Show drop-down menu filters the types of reports that are listed on the **Archived Reports** page.



## Note

---

Each report listed in the Report Type column is a hypertext link. Click on the hypertext link to access information about that report.

---

Additionally, interactive column headings can be used to sort the data in each column specific to your needs.

The appliance stores up to 12 instances of each scheduled report (up to 1000 reports). Archived reports are stored in the `/periodic_reports` directory on the appliance. Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 12 instances applies to each scheduled report with the same name and time range.

## 'Generate Report Now' Option

The **Generate Report Now** option on the **Web > Archived Reports** page allows you to generate on-demand data displays for each report type. To use this feature to generate a report, perform the following:

- 
- Step 1** On the Security Management appliance window, choose, **Web > Reporting > Archived Reports**.  
The Archived Reports page appears.
  - Step 2** Click on **Generate Report Now**.

**Figure 5-26**      **Generating an On-Demand Report****Generate Report**

**Step 3** From the Report type section, choose a report type from the drop-down list.

**Step 4** In the Title text field, type the name of the 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 5** From the **Time Range to Include** drop-down list, select a time range for the report data.

**Step 6** In the Format section, choose the format of the report.

Choices include:

- **PDF.** Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.
- **CSV.** Create an ASCII text file that contains the tabular data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.

**Step 7** From the Delivery Option section, choose the following:

- Archive the report by checking the **Archive Report** checkbox.

By choosing this, the report will appear on the Archived Reports page.

**Note**

Domain-Based Executive Summary reports cannot be archived.



- Check the **Email now to recipients** checkbox to email the report.
- In the text field, type in the recipient email addresses for the report.

**Step 8** Click **Deliver This Report** to generate the report.

---





# CHAPTER 6

## Tracking Email Messages

---

This chapter contains the following sections:

- [Tracking Service Overview, page 6-1](#)
- [About Setting Up Centralized Message Tracking, page 6-3](#)
- [Understanding Tracking Query Setup, page 6-3](#)
- [Running a Search Query, page 6-7](#)
- [Understanding Tracking Query Results, page 6-9](#)

## Tracking Service Overview

The tracking service of the Security Management appliance complements Email Security appliances. With the Security Management appliance, email administrators have a single place to track the status of messages that traverse any of their Email Security appliances.

The Security Management appliance makes it easy to find the status of messages that Email Security appliances process. Email administrators can quickly resolve help desk calls by determining the exact location of a message. With the Security Management appliance, an administrator can 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.

Instead of having to search through log files using `grep` or similar tools, you can use the flexible tracking interface of the Security Management appliance 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.
- **Attachment name:** You can search for messages based on an attachment name. Messages that contain at least one attachment with the queried name will appear in the search results.

For performance reasons, the names of files within attachments such as OLE objects or archives such as .ZIP files are not tracked.

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.
- **Event:** 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 Cisco IronPort message ID (MID).
- **Email Security appliance (host):** Narrow search criteria to particular Email Security appliances, or search across all managed appliances.

# About Setting Up Centralized Message Tracking

To set up centralized message tracking, see the following topics:

- [Enabling and Disabling Centralized Email Tracking on a Security Management Appliance, page 3-6.](#)
- [Disabling Access to Sensitive Information in Message Tracking, page 12-59](#)

## Understanding Tracking Query Setup

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

To search for a specific email message or group of messages that match specified criteria, perform the following:

- Step 1** On the Security Management appliance window, choose **Email > Message Tracking > Message Tracking**.

The Message Tracking page appears.

**Figure 6-1**      *The Message Tracking Page***Message Tracking**

| Search                                                                                                      |                                                                                                              |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| No Tracking Data is currently available. <span style="float: right;">Data in time range: 0% complete</span> |                                                                                                              |
| Envelope Sender: ?                                                                                          | Begins With <input type="text"/>                                                                             |
| Envelope Recipient: ?                                                                                       | Begins With <input type="text"/>                                                                             |
| Subject:                                                                                                    | Begins With <input type="text"/>                                                                             |
| Message Received:                                                                                           | <input type="radio"/> Last Day <input type="radio"/> Last Week <input checked="" type="radio"/> Custom Range |
| Start Date: <input type="text"/>                                                                            | Time: <input type="text"/> and End Date: <input type="text"/> Time: <input type="text"/> (GMT +0000)         |
| <a href="#">Advanced</a> Search messages using advanced criteria                                            |                                                                                                              |
| <input type="button" value="Clear"/>                                                                        | <input type="button" value="Search"/>                                                                        |

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

**Figure 6-2**      **Advanced Options for Tracking****Message Tracking**

| Search                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Envelope Sender: (?)                                                       | Begins With <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Envelope Recipient: (?)                                                    | Begins With <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Subject:                                                                   | Begins With <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Message Received:                                                          | <input checked="" type="radio"/> Last Day <input type="radio"/> Last Week <input type="radio"/> Custom Range<br>Start Date: <input type="text"/> 04/25/201             Time: <input type="text"/> 16:00             and             End Date: <input type="text"/> 04/26/201             Time: <input type="text"/> 16:08             (GMT +00:00)                                                                                                                                                                                                                                                                                                                                    |
| ▼ Advanced                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Sender IP Address:                                                         | <input type="text"/><br><input type="radio"/> Search rejected connections only <input checked="" type="radio"/> Search messages                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Attachment Name:                                                           | Begins With <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Message Event:                                                             | <i>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.</i><br><div> <input type="checkbox"/> Virus Positive               <input type="checkbox"/> Hard bounced<br/> <input type="checkbox"/> Spam Positive               <input type="checkbox"/> Soft bounced<br/> <input type="checkbox"/> Suspect Spam               <input type="checkbox"/> Quarantined as Spam<br/> <input type="checkbox"/> Delivered               <input type="checkbox"/> Currently in Outbreak Quarantine<br/> <input type="checkbox"/> DLP Violations           </div> |
| Message ID Header:                                                         | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| IronPort MID:                                                              | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| IronPort Host:                                                             | All Hosts <input type="button" value="v"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Query Settings: (?)                                                        | Query timeout: <input type="text"/> 1 minute <input type="button" value="v"/><br>Max. results returned: <input type="text"/> 250 <input type="button" value="v"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <input type="button" value="Clear"/> <input type="button" value="Search"/> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Note**

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

**Step 2**      Locate email messages you want to track.

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, user names, attachment names, 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, user names, attachment names, and domains.

If you use the alias table for alias expansion on your Email Security appliances, 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.

---

- **Message Received:** Specify a date and time range for the query using “Last Day,” “Last 7 Days,” or “Custom Range.” Use the “Last Day” option to search for messages within the past 24 hours, and use the “Last 7 Days” option to search for messages within the past full seven days, plus the time that has passed on the current day.

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. If you specify the current date and 23:59 as the end date and time, the query returns all data for the current date.

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 displayed in the local time of the appliance.

Messages appear in the results only after they have been logged on the Email Security appliance and retrieved by the Security Management appliance. Depending on the size of logs and the frequency of polling, there could be a small gap between the time when an email message was sent and when it actually appears in tracking and reporting results.

- **Sender IP Address:** Enter a sender IP address, and select whether to search messages or to search rejected connections only.



- **Message Event:** Select the events to track. Options are Virus Positive, Spam Positive, Suspect Spam, Delivered, DLP Violations (you can enter the name of a DLP policy and select violation severities), Hard Bounced, Soft Bounced, Currently in Outbreak Quarantine, 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.
- **Message ID Header and Cisco IronPort MID:** Enter a text string for the message ID header, the Cisco IronPort message ID (MID), or both.
- **Query Settings:** From the drop-down menu, select how long you want the query to run before it times out. Options are “1 minute,” “2 minutes,” “5 minutes,” “10 minutes,” and “No time limit.” Also, select the maximum number of results you want the query to return (up to 1000).
- **Attachment name:** Select Begins With, Is, or Contains, and enter an ASCII or Unicode text string for one Attachment Name to find.

**Step 3** Click **Search**.

---

## Running a Search Query

To search for messages by running a query, perform the following:

**Step 1** On the Security Management appliance window, choose **Email > Message Tracking > Message Tracking**.

**Step 2** Complete the desired search fields.

For more information about the available search fields, see the [“Understanding Tracking Query Setup” section on page 6-3](#).

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 3** Click **Search** to submit the query.

The query results appear at the bottom of the page. Each row corresponds to an email message.

**Figure 6-3 Message Tracking Query Results**

| Results                                                                                                                                                                                                                           |                                   |                |                               | Items per page 20                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|----------------|-------------------------------|-----------------------------------------|
| Displaying 1 — 20 of 197 items.                                                                                                                                                                                                   |                                   | Page 1 of 10   |                               | « Previous   1   2   3   4   5   Next » |
| 1                                                                                                                                                                                                                                 | 26 Apr 2011 10:02:21 (GMT -07:00) | MID: 114390707 | HOST: Security1 (192.0.2.255) | <a href="#">Show Details</a>            |
| SENDER: joeshmoe@test.com<br>RECIPIENT: test1@ironport.com<br>SUBJECT: Successfull Order 984890<br>LAST STATE: Message 114390709 to test1@ironport.com received remote SMTP response 'sent'.<br><a href="#">Order details.zip</a> |                                   |                |                               |                                         |
| 2                                                                                                                                                                                                                                 | 26 Apr 2011 10:01:10 (GMT -07:00) | MID: 114390700 | HOST: Security1 (192.0.2.255) | <a href="#">Show Details</a>            |
| SENDER: user1@test.com<br>RECIPIENT: test2@ironport.com<br>SUBJECT: Successfull Order 807915<br>LAST STATE: Message 114390702 to test2@ironport.com received remote SMTP response 'sent'.<br><a href="#">Order details.zip</a>    |                                   |                |                               |                                         |
| 3                                                                                                                                                                                                                                 | 26 Apr 2011 09:56:02 (GMT -07:00) | MID: 114390628 | HOST: Security1 (192.0.2.255) | <a href="#">Show Details</a>            |
| SENDER: jsmith@smith.com<br>RECIPIENT: joeshmoe@ironport.com<br>SUBJECT: Successfull Order 872528<br>LAST STATE: Message 114390629 quarantined to Virus. Anti-Virus verdict VIRAL.<br><a href="#">Order details.zip</a>           |                                   |                |                               |                                         |
| 4                                                                                                                                                                                                                                 | 26 Apr 2011 09:55:15 (GMT -07:00) | MID: 114390621 | HOST: Security1 (192.0.2.255) | <a href="#">Show Details</a>            |

Your search criteria are highlighted in each row.

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

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, narrow the result set by clicking a value within a row in the list of results. Clicking a value adds the parameter value as a condition in the search. For example, if the query results include messages from multiple dates, 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.

Use the following parameter values to refine the search:

- Date and time
- Message ID (MID)
- Host (the Email Security appliance)
- Sender
- Recipient
- The subject line of the message, or starting words of the subject

**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 **Clear** 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  $\mathfrak{J}$  and you specify that the subject begins with  $\mathfrak{T}$ , the query returns a message only if both conditions are true for that message.



**Note** Messages with 50 or more recipients will not appear in tracking query results. This issue will be resolved in a future release of AsyncOS.

For each message, the following information is shown: date/time, sender, recipient, subject, last state, any attachments that were included in the message, Cisco IronPort message ID (MID), and Cisco IronPort host (the Email Security appliance). To view detailed information about a message, click the **Show Details** link for that message. For more information, see the [“Message Details” section on page 6-10](#).


**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 **Show Details** for any item in the search results list. A new window opens with the message details.

The message details include the following sections:

- [Envelope and Header Summary, page 6-10](#)
- [Sending Host Summary, page 6-11](#)
- [Processing Details, page 6-11](#)

### 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:** 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 Email Security appliances are not configured to record the subject lines in log files.

**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.

**Cisco IronPort Host:** Email Security appliance that processed the message.

**SMTP Auth User ID:** SMTP authenticated user name 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.

## 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.

If the message was delivered, the details of the delivery appear here.

The last recorded event is highlighted in the processing details.

## DLP Matched Content

This section displays content that violates Data Loss Prevention (DLP) policies.

Because this content typically includes sensitive information, such as corporate confidential information or personal information including credit card numbers and health records, you may want to disable access to this

content for users who do not have Administrator-level access to the appliance. See [Disabling Access to Sensitive Information in Message Tracking](#), page 12-59.



## CHAPTER 7

# Managing the Cisco IronPort Spam Quarantine

---

This chapter contains the following sections:

- [Understanding the Cisco IronPort Spam Quarantine, page 7-1](#)
- [Configuring Cisco IronPort Spam Quarantine Settings, page 7-3](#)
- [Configuring End User Access and Notifications, page 7-7](#)
- [Setting Up Email Security Appliances to Forward Spam, page 7-12](#)
- [Managing Messages in the Cisco IronPort Spam Quarantine, page 7-15](#)
- [Enabling the End User Safelist/Blocklist Feature, page 7-19](#)
- [Using End User Safelists and Blocklists, page 7-23](#)

## Understanding the Cisco IronPort Spam Quarantine

A Cisco IronPort Spam Quarantine is a special kind of quarantine that is used to hold spam and suspected spam messages for end users. (End users are mail users, not AsyncOS users.) A *local* Cisco IronPort Spam Quarantine resides on an Email Security gateway appliance. You can also have messages sent to an *external* Cisco IronPort Spam Quarantine, which resides on a separate Cisco IronPort appliance — typically a Security Management appliance.

**Note**

A *system quarantine* resides on an Email Security appliance and holds quarantined messages based on various actions that AsyncOS performs, such as content filtering, anti-virus scanning, and applying Outbreak Filters.

The Cisco IronPort Spam Quarantine provides a safeguard mechanism for organizations that are concerned about “false positives” — that is, legitimate email messages that are quarantined or deleted as spam. With the Cisco IronPort Spam Quarantine, you can allow end users and administrators to review messages that are flagged as spam before making a final determination. In addition, if you enable the safelist/blocklist feature, end users can exercise control over the messages that are marked as spam.

**Note**

You can implement end user access to the Cisco IronPort Spam Quarantine only for specified users or groups of users. Also, after you initially implement end user access, you might later decide to disable access if end users rarely view and release messages in the quarantine.

You can configure AsyncOS to send a notification email to end users, informing them of quarantined spam and suspected spam messages. The notification contains a summary of the messages currently in the Cisco IronPort Spam Quarantine for that user. The user can view the messages and decide whether to have them delivered to the Email Inbox or delete them. Users can also search through their quarantined messages. Users can access the quarantine through the notification message, or they can access the quarantine directly by using a web browser. (Direct end user access to the quarantine requires authentication. For more information, see the [“Configuring End User Quarantine Access”](#) section on [page 7-8](#)).

By default, the Cisco IronPort Spam Quarantine is self-maintaining. AsyncOS periodically deletes mail from the Cisco IronPort Spam Quarantine to prevent old messages from consuming all of the quarantine space.

All administrator-level users (such as the default admin user) can access and modify the Cisco IronPort Spam Quarantine. AsyncOS operator users and users to whom you assign Spam Quarantine access via a custom role can view and manage the quarantine content, but they cannot change the quarantine settings. Mail end users can access their own messages in the quarantine if you enable end user access to the Cisco IronPort Spam Quarantine.



# Configuring Cisco IronPort Spam Quarantine Settings

Before you edit the Cisco IronPort Spam Quarantine settings on a Security Management appliance, you need to enable the Cisco IronPort Spam Quarantine service on the Security Management appliance. For information about how to enable the service, see the [“Enabling and Disabling the Cisco IronPort Spam Quarantine on a Security Management Appliance”](#) section on page 3-8.

To edit the Cisco IronPort Spam Quarantine settings:

- 
- Step 1** On the Security Management appliance window, choose **Management Appliance > Centralized Services > Spam Quarantine**
  - Step 2** Click the **Edit Settings** in the Cisco IronPort Spam Quarantine Settings section. The Edit Cisco IronPort Spam Quarantine page appears.

**Figure 7-1**      **Editing the Cisco IronPort Spam Quarantine Settings****Edit IronPort Spam Quarantine**

| Spam Quarantine Settings                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Enable IronPort Spam Quarantine                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Quarantine IP Interface:                                                                                                                                                                                                                                                                              | Management ▾                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Quarantine Port:                                                                                                                                                                                                                                                                                      | 11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Deliver Messages Via:                                                                                                                                                                                                                                                                                 | <p>Notifications and released messages will be delivered by the server(s) specified below.</p> <p>Primary Server: 127.0.0.1 Port: 25<br/> <small>IronPort Appliance or SMTP Server IP Address</small></p> <p>Alternative Server: 127.0.0.1 Port: 25</p> <p><small>Note: You must configure your destination server(s) to accept mail from this host. If you are delivering to an IronPort Appliance, it must be configured to direct spam to this appliance. See the IronPort documentation for more information.</small></p> |
| Schedule Delete After:                                                                                                                                                                                                                                                                                | <input checked="" type="radio"/> 14 days<br><input type="radio"/> Do not schedule delete                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Default Language:                                                                                                                                                                                                                                                                                     | English/United States [en-us] ▾                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Notify IronPort Upon Message Release:                                                                                                                                                                                                                                                                 | <input type="checkbox"/> Send a copy of released messages to IronPort for analysis(recommended)                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Spam Quarantine Appearance:                                                                                                                                                                                                                                                                           | <p>Current Logo:  <b>IRONPORT</b> Spam Quarantine</p> <p> <input checked="" type="radio"/> Use Current Logo<br/> <input type="radio"/> Use IronPort Spam Quarantine Logo<br/> <input type="radio"/> Upload Custom Logo: <input type="text"/> <input type="button" value="Browse..."/><br/> <small>Maximum size 500w x 50h pixels</small> </p> <p>Login Page Message: <input type="text"/></p>                                                |
| Administrative Users                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <small>You have no 'operator' users defined in your system.<br/>           Go to System Administration &gt; to configure users.<br/>           Members of the 'Administrator' group have full access to Quarantines and will automatically be granted access to the IronPort Spam Quarantine.</small> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Step 3** In the **Quarantine IP Interface** section, specify the appropriate IP interface and port for the quarantine from the drop-down list.

By default, the quarantine uses the Management interface and port 6025. The IP interface is the interface on the Security Management appliance that is configured to listen for incoming mail. The quarantine port is the port number that the sending appliances use in their external quarantine settings.

**Step 4** In the **Deliver Messages Via** section, type the primary and alternate destinations for delivering mail in the corresponding text fields.

A destination could be an SMTP or groupware server or another appliance.

**Step 5** In the Schedule Delete After section, specify the number of days to hold messages before deleting them.

Alternatively, select the **Do not schedule a delete** radio button to disable scheduled deletions. It is recommended that you configure the quarantine to schedule deletions. When the quarantine fills to capacity, it deletes the oldest messages first.

**Step 6** In the Default Language section, specify a default language.

This is the language that end users see when they access the Cisco IronPort Spam Quarantine.

**Step 7** (Optional) In the **Notify Cisco IronPort upon Message Release**, check the checkbox to send a copy of released messages to Cisco IronPort for analysis.

It is recommended that you configure the quarantine to submit released messages for analysis.

**Step 8** (Optional) In the Spam Quarantine Appearance section, customize the page that end users access when they view the quarantine.

Choices include:

- Use Current logo
- Use Cisco IronPort Spam Quarantine logo
- Upload Custom logo

If you choose ‘Upload Custom logo’, the logo appears at the top of the Cisco 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.

**Step 9** (Optional) In the **Login Page Message** text field, type in a login page message. The message appears to end users when they are prompted to log in to the quarantine.

**Step 10** Optionally, modify the list of users authorized to view the Cisco IronPort Spam Quarantine. For more information, see [Configuring Administrative Users for Cisco IronPort Spam Quarantine](#), page 7-6.

**Step 11** Optionally, end user access, and spam notification settings. For more information, see [Configuring End User Access and Notifications](#), page 7-7.

**Step 12** Submit and commit your changes.

## Configuring Administrative Users for Cisco IronPort Spam Quarantine

You can distribute responsibility for managing messages in the Cisco IronPort Spam Quarantine to other people. You must use the procedure in this section to enable these people to access this functionality.

Users can manage messages in the Spam Quarantine if they are assigned the Operator, Read-Only Operator, Help Desk, or Guest roles, or if they are assigned a custom user role that includes access to the Spam Quarantine.

Administrator-level users, including the default admin user and Email Administrator users, can always access the Spam Quarantine and do not need to be associated with the Spam Quarantine feature using this procedure.



### Note

Non-Administrator-level users can access messages in the Spam Quarantine, but they cannot edit the quarantine settings. Administrator-level users can access messages and edit the settings.

To enable users to manage the Spam Quarantine:

- Step 1** Make sure you have created users and assigned them a user role with access to the Spam Quarantine. For information, see [About Distributing Administrative Tasks, page 12-40](#).
- Step 2** On the Security Management appliance, choose **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 3** Click **Enable** or **Edit Settings** in the Spam Quarantine Settings section. The Edit Spam Quarantine page appears.
- Step 4** In the Administrative Users area of the Spam Quarantine Settings section, click the selection link for Local Users, Externally Authenticated Users, or Custom User Roles.
- Step 5** Select the users to whom you want to grant access to view and manage messages in the Spam Quarantine.
- Step 6** Click OK.
- Step 7** Repeat if needed for each of the other types of Administrative Users listed in the section (Local Users, Externally Authenticated Users, or Custom User Roles).

**Step 8** Click **Submit** and then commit your changes.

## Configuring End User Access and Notifications

In addition to the basic Cisco IronPort Spam Quarantine settings, you can configure other settings for the quarantine. The additional settings appear below the Spam Quarantine Settings section of the Edit Cisco IronPort Spam Quarantine page.

You can configure the following additional settings:

- **End user access to the quarantine:** For more information, see [Configuring End User Quarantine Access, page 7-8](#).
- **Spam notifications:** For more information, see [Enabling Spam Notifications, page 7-9](#).

To access the additional settings, select Management Appliance > Centralized Services > Spam Quarantine, and then click the **Edit Settings** button in the Cisco IronPort Spam Quarantine Settings section. Scroll down on the Edit Cisco IronPort Spam Quarantine page to view the additional settings.

**Figure 7-2** *Editing Additional Settings for the Cisco IronPort Spam Quarantine*

| End-User Quarantine Access                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Enable End-User Quarantine Access                                                                                                                                            |
| <i>Enabling this feature allow end-users to access and manage their suspected spam quarantine. Users with access will be able to view, search, release and delete messages from their quarantine.</i> |

| Spam Notifications                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Enable Spam Notification                                                                                                                                 |
| <i>Enabling Spam Notification causes email notifications to be sent in digest format, listing a summary of all messages quarantined since the last notification. See example.</i> |

Cancel
Submit



### Note

You can configure one of the additional settings, but not the others. For example, to provide access only upon request or only to specified users, you might configure end user access, but not spam notifications.

## Configuring End User Quarantine Access

To configure end user access to the Cisco IronPort Spam Quarantine:

- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 2** Click the **Edit Settings** in the Cisco IronPort Spam Quarantine Settings section. The Edit Cisco IronPort Spam Quarantine page appears.
- Step 3** Check the Enable End-User Quarantine Access check box on the **Edit Cisco IronPort Spam Quarantine** page.

**Figure 7-3** *Enabling End User Access to the Cisco IronPort Spam Quarantine*

- Step 4** Specify the method to authenticate end users when they attempt to view their quarantined messages. You can use mailbox authentication, LDAP authentication, or none.

- **Mailbox authentication:** For sites without an LDAP directory for authentication, the quarantine can validate users' email addresses and passwords against a standards-based IMAP or POP server that holds their mailboxes. When logging in to the web UI, users enter their full email address and mailbox password. The quarantine uses this information to log in to the mailbox server as the user. If the login is successful, the user is authenticated and the quarantine logs out of the mailbox server without making any changes to the user's Inbox. Mailbox authentication is recommended for sites that do not use an LDAP directory. However, mailbox authentication cannot provide a user with quarantined messages that were sent to multiple email aliases.

Select the type of mailbox server (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 (for example, company.com) to append to unqualified user names.

If the POP server advertises APOP support in the banner, then for security reasons (namely, to avoid sending the password in the clear) the appliance uses APOP only. If APOP is not supported for some users, then the POP server should be reconfigured so that it does not advertise APOP.

- **LDAP:** If you do not have an LDAP server or an active end user authentication query set up, choose **Management Appliance > System Administration > LDAP** to configure your LDAP server settings and end user authentication query string. For information about configuring LDAP authentication, see [Creating the LDAP Server Profile, page 10-3](#).
- **None:** You can allow end user access to the Cisco IronPort Spam Quarantine without enabling authentication. In this case, users can access the quarantine by clicking a link in the notification message, and the system does not use mailbox or LDAP authentication.

**Step 5** Specify whether or not to display message bodies before messages are released from the quarantine. If this check box is selected, users cannot view the message body through the Cisco IronPort Spam Quarantine page. Instead, to view a quarantined message, users must release the message and view it in their mail application (for example, Microsoft Outlook). You can use this feature for policy and regulation compliance — for example, if a regulation requires that all viewed email be archived.

**Step 6** Click **Submit** and then click **Commit** to commit your changes.

---

## Enabling Spam Notifications

Spam notifications are email messages sent to end users when they have messages in the Cisco IronPort Spam Quarantine. Notifications contain a list of quarantined spam or suspected spam for the user. Notifications also include a link for users to view their quarantined messages. Once enabled, notifications are sent according to the schedule that you specify on the Edit Cisco IronPort Spam Quarantine page.

Spam notifications can provide a way for end users to log in to the quarantine without using LDAP or mailbox authentication. Users access the quarantine through the email notifications that they receive (if notifications are enabled for the quarantine). Clicking a message subject logs the user in to the web UI for the quarantine.

**Note**

This login method does not display quarantined messages for other aliases that the end user may have. Also, if the notification was sent to a distribution list that was expanded after the appliance processed it, then multiple recipients might have access to the same quarantine for the list.

Because of the way the 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, navigate to Management Appliance > System Administration > LDAP to configure your LDAP server settings and alias consolidation query string.** For more information, see [Configuring End User Access and Notifications, page 7-7](#).

To configure spam notifications:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Spam Quarantine**.
  - Step 2** Click **Edit Settings** in the Cisco IronPort Spam Quarantine Settings section. The Edit Cisco IronPort Spam Quarantine page appears.
  - Step 3** Check the **Enable Spam Notification** check box to enable spam notification.



Figure 7-4 Configuring Spam Notifications

| Spam Notifications                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Enable Spam Notification |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| From Address:                                                | "friendly name" (optional) <username@hostname><br><small>(example: "Email Administrator" &lt;notify@company.com&gt;)</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Subject:                                                     | IronPort Spam Quarantine Notification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Title:                                                       | IronPort Spam Quarantine Notification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Message Body: ?                                              | <div> <p>The message(s) below have been blocked by your administrator as suspected spam.</p> <p>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).</p> <p>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%.</p> <p><a href="#">Preview Message</a></p> </div> <div> <b>Message Variables</b><br/>           New Message Count<br/>           Total Message Count<br/>           ..<br/>           Days Until Message Expires<br/>           Quarantine URL<br/>           Username<br/>           New Message Table         </div> |
| Message Format:                                              | HTML (recommended)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Deliver Bounce Message To:                                   | <input type="text" value="(e.g. mybounceaddress@company.com)"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Consolidate Notifications:                                   | <input type="checkbox"/> Consolidate notifications sent to the same LDAP user at different addresses<br><small>This setting uses the LDAP Alias Consolidation Query configured at System Administration &gt; LDAP.</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Notification Schedule:                                       | <input type="radio"/> Monthly (Sent the 1st of each month at 12am)<br><input checked="" type="radio"/> Weekly <b>Monday</b> (Sent at 12am)<br><input type="radio"/> Daily (weekdays) <div> <input type="checkbox"/> 12 <input type="checkbox"/> 3 <input type="checkbox"/> 6 <input type="checkbox"/> 9 AM<br/> <input type="checkbox"/> 12 <input type="checkbox"/> 3 <input type="checkbox"/> 6 <input type="checkbox"/> 9 PM           </div>                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- Step 4** Enter a From address for the notifications. Users may want to add this address to a “whitelist” supported by their email client.
- Step 5** Enter a subject for the notification.
- Step 6** Enter a customized title for the notification.
- Step 7** 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%)**: number of new messages since the user’s last login
- **Total Message Count (%total\_message\_count%)**: 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 the quarantine and view messages
- **Username (%username%)**
- **New Message Table (%new\_quarantine\_messages%):** list of new messages in the quarantine for the user

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

- Step 8** Select a message format (HTML, Text, or HTML/Text).
  - Step 9** Specify a bounce address. Bounced notifications are sent to this address.
  - Step 10** Optionally, you can consolidate messages sent to the same LDAP user at different addresses.
  - Step 11** Set the notification schedule. You can configure the notifications to be sent once a month, once a week, or at specified times during the day (weekdays only or including weekends).
  - Step 12** Click **Submit** and then click **Commit** to commit your changes.
- 

## Setting Up Email Security Appliances to Forward Spam

After you configure the Cisco IronPort Spam Quarantine on the Security Management appliance, you need to set up the Email Security appliances in your system to forward spam or suspected spam to the Security Management appliance.

Setting up the Email Security appliances to forward spam involves the following tasks:

- **Configuring external quarantine settings:** In the external quarantine settings on the Email Security appliances, you need to specify the Security Management appliance name and connection information for the Cisco IronPort Spam Quarantine. For more information, see [Configuring External Quarantine Settings, page 7-13](#).

- **Adding or updating managed appliances:** You need to add or update the Email Security appliances as managed appliances on the Security Management appliance, and you need to select the option to quarantine spam from the Email Security appliances. For more information, see [Adding and Updating Managed Appliances and Using the Quarantine Spam Option](#), page 7-14.

## Configuring External Quarantine Settings

If you want Email Security appliances to use the Cisco IronPort Spam Quarantine on the Security Management appliance, you need to configure the external quarantine settings on the Email Security appliances.



### Note

If a different external spam quarantine was previously configured for the Email Security appliances, first disable the external spam quarantine setting.

To configure the external quarantine settings, complete the following steps **on each** Email Security appliance:

- Step 1** On the Security Services > External Spam Quarantine page, click the **Configure** button.
- Step 2** Select the check box to enable the external spam quarantine.
- Step 3** Enter the name of the Cisco IronPort Spam Quarantine. Alternatively, you can enter the name of the Security Management appliance where the quarantine resides.
- Step 4** Enter the IP address for the Management interface of the Security Management appliance.
- Step 5** Enter the port number to use for delivering spam and suspected spam. The default is 6025. The port number that you enter here must match the quarantine port number that you entered on the Edit Cisco IronPort Spam Quarantine page of the GUI for the Security Management appliance. For more information, see [Configuring Cisco IronPort Spam Quarantine Settings](#), page 7-3.

- Step 6** Optionally, select the check box to enable the safelist/blocklist feature. If you enable the safelist/blocklist feature, select whether to quarantine or delete messages from blocklisted senders. For more information about the safelist/blocklist feature, see [Enabling the End User Safelist/Blocklist Feature, page 7-19](#).
- Step 7** Click **Submit** and then click **Commit** to commit your changes.
- 

## Adding and Updating Managed Appliances and Using the Quarantine Spam Option

If you want your Email Security appliances to use the Cisco IronPort Spam Quarantine on a Security Management appliance, you need to add them as managed appliances on the Security Management appliance. Or, if the Email Security appliances have already been added as managed appliances, you need to update the managed appliance configuration to use the quarantine spam option.

On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances** to add managed Email Security appliances. For more information about adding managed appliances, see [Adding Managed Appliances, page 3-10](#).



### Caution

When you add a managed appliance, be sure to select the option to quarantine spam from the appliance.

---

If an Email Security appliance already exists as a managed appliance on the Security Management appliance, then you need to update the managed appliance configuration to use the quarantine spam option.

To update the managed appliance configuration to use the quarantine spam option:

---

- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 2** In the list of security appliances, click the name of the Email Security appliance.
- Step 3** On the Edit Appliance: <appliance\_name> page, select the option to quarantine spam from the appliance, as shown in [Figure 7-5](#).

**Figure 7-5** *Editing a Managed Appliance to Quarantine Spam***Edit Appliance: example.srv**

| Security Appliance    |                                                                                                                                                                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Name:       | example.srv                                                                                                                                                                                                                                                       |
| IP Address:           | 111.11.1.11                                                                                                                                                                                                                                                       |
| Centralized Services: | <input checked="" type="checkbox"/> Quarantine spam from this appliance<br><input type="checkbox"/> Centralized reporting: all available host licenses in use<br><input type="checkbox"/> Centralized tracking: all available host licenses in use                |
| File Transfer Access: | Not configured.<br><small>File transfer access via ssh is required for transfer of reporting data, message tracking data, and quarantine Safelist/Blocklist data</small><br><a href="#">Test Configuration</a> <a href="#">Configure File Transfer Access....</a> |

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

**Step 4** Click **Submit** and then click **Commit** to commit your changes.

## Managing Messages in the Cisco IronPort Spam Quarantine

This section explains how administrators can manage messages in the Cisco IronPort Spam Quarantine. When an administrator views the quarantine, all of the messages contained in the quarantine are available.



### Note

The GUI for viewing and managing messages is slightly different for end users who access the Cisco IronPort Spam Quarantine. For information about the end user GUI, access the Cisco IronPort Spam Quarantine as an end user, and view the online help.

As an administrator, you can perform the following actions on messages in the Cisco IronPort Spam Quarantine:

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

To access messages in the Cisco IronPort Spam Quarantine perform the following:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 2** Click the Cisco IronPort Spam Quarantine link.  
The Spam Quarantine Search page appears.

**Figure 7-6 Spam Quarantine Search Page**

#### Spam Quarantine Search

- Step 3** Click **Submit** and then click **Commit** to commit your changes.
- 

## Searching for Messages in the Cisco IronPort Spam Quarantine

To search the messages in the Cisco IronPort Spam Quarantine, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Email > Message Quarantine > Spam Quarantine**.
- Step 2** On the search form, enter the dates to search. You can search messages from the current day or the past week, or you can click the calendar icons to select a date range.
- Step 3** Optionally, specify a text string for the From address, To address, or message subject. Select whether the search results contain, do not contain, match exactly, start with, or end with the value that you enter.

- Step 4** Optionally, specify an envelope recipient. Select whether the search results contain, do not contain, match exactly, start with, or end with the value that you enter.

The envelope recipient is the address of the email message recipient as defined in the “RCPT TO” SMTP command. The envelope recipient is also sometimes called the “Recipient To” address or the “Envelope To” address.

- Step 5** Click **Search**.

Messages that match the search criteria appear below the Search section of the page.

---

## Searching Large Message Collections

If a large number of messages are stored in the Cisco IronPort Spam Quarantine and the search terms are not narrowly defined, a query may take a long time to display the search results, or the query may time out.

You are prompted to confirm whether you want to resubmit the search.



### Note

Running multiple large searches simultaneously can adversely affect the performance of the appliance.

---

## Viewing Messages in the Cisco IronPort Spam Quarantine

The message list shows messages in the Cisco IronPort Spam Quarantine. You can select how many messages appear on a page. You can sort the display by clicking the column headings. Click a column heading a second time to reverse the sorting.

Click the subject of a message to view the message, including the body and headers. The first 20K of the message appears on the Message Details page. If the message is longer, it is truncated at 20K. Click the link at the bottom of the page to view the rest of the message.

From the Message Details page, you can select Delete to delete a message or select Release to release the message from the quarantine. Releasing a message causes it to be delivered.

## Viewing HTML Messages

The Cisco IronPort Spam Quarantine attempts to render an approximation of HTML-based messages. Images do not appear.

## Viewing Encoded Messages

Base64 encoded messages are decoded and then appear.

## Delivering Messages in the Cisco IronPort Spam Quarantine

To release messages for delivery, select the check box next to the messages and click **Release**.

Select the check box in the heading row to select all of the messages 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 specified period of time. You can also delete messages from the Cisco IronPort Spam Quarantine manually.

To delete specific messages, select the check box next to the messages you want to delete and then click **Delete**. Select the check box in the heading row to select all of the messages displayed on the page.

To delete all of the messages in the Cisco IronPort Spam Quarantine, disable the quarantine (see [Enabling and Disabling the Cisco IronPort Spam Quarantine on a Security Management Appliance, page 3-8](#)), and then click the **Delete All** link on the **Management Appliance > Centralized Services > Spam Quarantine** page.



## Enabling the End User Safelist/Blocklist Feature

You can allow end users to create safelists and blocklists to better control which email messages are treated as spam. Safelists allow a user to ensure that mail from specified users and domains is never treated as spam. Blocklists ensure that mail from other users and domains is 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**

A safelist or blocklist setting does not prevent the Email Security appliance from scanning a message for viruses or determining if the message meets the criteria for a content-related mail policy. If a message is sent from a safelist member, it might not be delivered to the end user depending on other scanning settings.

When a user adds an entry to a safelist or blocklist, the entry is stored in a database on the Security Management appliance and periodically updated and synchronized on all related Email Security appliances. For information about synchronization, see [Synchronizing Safelist and Blocklist Settings and Databases, page 7-22](#). For information on backing up the database, see [Backing Up and Restoring the Safelist/Blocklist Database, page 7-21](#).

The safelists and blocklists are created and maintained by end users. However, an administrator enables the feature and configures delivery settings for email messages that match entries in the blocklist. Because the safelists and blocklists are related to the Cisco IronPort Spam Quarantine, delivery behavior is also contingent on other anti-spam settings. A message might skip anti-spam scanning based on the processing that occurs before the message reaches the Email Security Manager in the email pipeline. For more information about message processing, see “Understanding the Email Pipeline” in the *Cisco IronPort AsyncOS for Email User Guide*.

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.

For more information about delivery of safelist/blocklist messages, see [Message Delivery for Safelists and Blocklists](#), page 7-22.

## Enabling and Configuring Safelist/Blocklist Settings

Before you can enable the safelist/blocklist feature, you must enable the Cisco IronPort Spam Quarantine on the appliance. For more information about enabling the Cisco IronPort Spam Quarantine, see [Enabling and Disabling the Cisco IronPort Spam Quarantine on a Security Management Appliance](#), page 3-8.

To enable and configure the safelist/blocklist feature on a Security Management appliance:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Spam Quarantine**.
  - Step 2** Click **Enable** in the End-User Safelist/Blocklist section.
  - Step 3** Click **Edit Settings** in the End-User Safelist/Blocklist section.
  - Step 4** Verify that the **Enable End User Safelist/Blocklist Feature** check box is checked.
  - Step 5** Specify the maximum number of list items per user. This value is the maximum number of addresses and domains that a user can include in each safelist and blocklist. The default is 100.
- 

**Note** If you allow a large number of list entries per user, system performance might be adversely affected.
- 
- Step 6** Select the update frequency. This value determines how often AsyncOS updates the safelist/blocklist databases on the Email Security appliances in the system. The default is every two hours for M10, M600, and M650 appliances. The default is every four hours for M1000 and M1050 appliances.
  - Step 7** Click **Submit** and then click **Commit** to commit your changes.
-

## Backing Up and Restoring the Safelist/Blocklist Database

To maintain a backup of the safelist/blocklist database, the Security Management appliance enables you to save the database as a .csv file. The .csv file is maintained separately from the XML configuration file that contains the appliance configuration settings. If you upgrade your appliance or run the System Setup Wizard, first back up the safelist/blocklist database to the .csv file.



### Note

You can edit the .csv file and then upload it to modify individual end users' safelists and blocklists.

When you back up the database, the appliance saves the .csv file to the `/configuration` directory using the following naming convention:

*slbl-<serial number>-<timestamp>.csv*

From the GUI, you can use the following method to back up and restore the database:

- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > Configuration File**.
- Step 2** Go to the End-User Safelist/Blocklist Database section.

- Step 3** Click **Backup Now** to back up the database to a .csv file.
- Step 4** Click **Select File to Restore** to restore the database.  
The appliance displays a list of backup files that are stored in the `/configuration` directory.
- Step 5** Select the Safelist/Blocklist backup file that you want to restore, and click **Restore**.

## Synchronizing Safelist and Blocklist Settings and Databases

With the Security Management appliance, you can easily synchronize the safelist/blocklist databases on all managed appliances.

**Note**

Before you can synchronize safelist/blocklist databases, you need to enable the safelist/blocklist feature and add at least one managed appliance to the Security Management appliance. For more information about adding managed appliances, see [Adding Managed Appliances, page 3-10](#).

To synchronize safelist/blocklist databases, click the **Synchronize All Appliances** button on the Management Appliance > Centralized Services > Spam Quarantine page.

If you use the centralized management feature to configure multiple 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 using FTP to access appliances, see Appendix A, 'Accessing the Appliance,' on page 1.

## Message Delivery for Safelists and Blocklists

When you enable safelists and blocklists, the Email Security appliance scans the messages against the safelist/blocklist database immediately before anti-spam scanning. If the appliance detects a sender or domain that matches an end user's safelist/blocklist setting, the message is splintered if it has multiple recipients with different safelist/blocklist settings. For example, sender X sends a message to both recipient A and recipient B. Recipient A has safelisted sender X, but recipient B has no entry for the sender in either the safelist or the 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 it skips anti-spam scanning. 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, and so forth), and they are subject to any configured settings.

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.

**Note**

You specify blocklist actions in the external spam quarantine settings on the Email Security appliance. For more information, see [Configuring External Quarantine Settings, page 7-13](#).

If you configure the blocklist action to quarantine messages, the message is scanned and eventually quarantined. If you configure the blocklist action to delete messages, the message is deleted immediately after safelist/blocklist scanning.

## Troubleshooting Safelists and Blocklists

End users maintain their own safelists and blocklists. Administrators can access an end user's safelist or blocklist by logging in to the end user account with the user's login and password. Alternatively, an administrator can download a backup version of the safelist/blocklist database to edit individual users' lists.

To troubleshoot issues with safelists and blocklists, you can view the log files or system alerts.

When an email message is blocked due to safelist/blocklist settings, the action is logged in the ISQ\_logs or the anti-spam log files.

Alerts are sent out when the database is created and updated, or if there are errors in modifying the database or running the safelist/blocklist processes.

For more information about alerts, see [Managing Alerts, page 12-76](#).

For more information about log files, see Chapter 13, 'Logging,' on page 1.

## Using End User Safelists and Blocklists

End users can create safelists to ensure that messages from specified senders are never treated as spam, and they can use blocklists to ensure that messages from specified senders are always treated as spam. For example, an end user might

receive unwanted email from a mailing list. The user can add this sender to the user's blocklist to prevent email messages from the sender from being delivered. On the other hand, an end user might find that email messages from a legitimate sender are sent to the Cisco IronPort Spam Quarantine, but those email messages should not be treated as spam. To prevent mail from that sender from being quarantined, the user can add the sender to the user's safelist.

**Note**

Safelist/blocklist settings are contingent on other settings configured by the system administrator. For example, a safelisted message may not be delivered if it is determined to be virus positive, or if the administrator determines that the content does not conform to company email policies.

## Accessing Safelists and Blocklists

To access safelists and blocklists, end users whose accounts are authenticated using LDAP or mailbox authentication (IMAP or POP) must log in to their accounts on the Cisco IronPort Spam Quarantine. The end users must log in to their accounts even if they are accustomed to accessing messages through a spam notification (which typically does not require LDAP or mailbox authentication). If the end user authentication is set to None, end users do not need to log in to their accounts to access safelist/blocklist settings.

## Adding Entries to Safelists and Blocklists

Entries can be added to safelists and blocklists using the following formats:

- user@domain.com
- server.domain.com
- domain.com

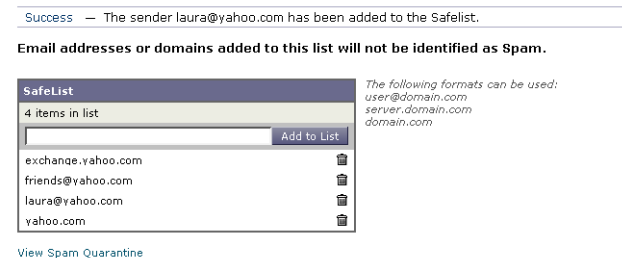
End users cannot add a sender or domain to both their safelist and their blocklist at the same time. However, if they add a domain to a safelist and a user in that domain to the blocklist (or vice versa), the appliance applies both rules. For example, if the end user adds *example.com* to the safelist, and adds *george@example.com* to the blocklist, the appliance delivers all mail from *example.com* without scanning for spam, but it treats mail from *george@example.com* as spam.

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

## Working with Safelists

End users can add senders to safelists in two ways. From the Cisco IronPort Spam Quarantine, they can manually add a sender to the safelist by clicking the Options menu in the upper-right corner of the GUI and then selecting Safelist.

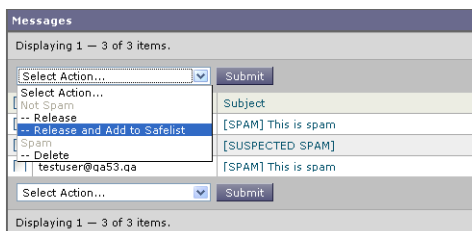
**Figure 7-7** *Safelist in End User Quarantine*



Add an email address or domain to the list, and click **Add to List**.

End users can also add senders to the safelist if the message has been sent to the Cisco IronPort Spam Quarantine. If the message from a particular sender is held in the Cisco IronPort Spam Quarantine, the end user can select the check box next to the message, and choose “Release and Add to Safelist” from the drop-down menu.

**Figure 7-8** *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.



#### Note

End users can also use the spam notification message to release messages. Click the Not Spam link to release a particular message. End users also have the option to add senders to their safelists.

## Working with Blocklists

End users can use blocklists to prevent the delivery of mail from specified senders. To add senders to a blocklist, the end user selects Options > Blocklist from the end user quarantine.

**Figure 7-9 Adding Senders to a Blocklist**



From the end user quarantine, the end user enters an email address or domain in the field, and clicks **Add to List**.

When the Email Security 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 might be deleted or quarantined, depending on the blocklist action setting.





## CHAPTER 8

# Managing Web Security Appliances

---

This chapter contains the following sections:

- [Overview of Managing Web Security Appliances, page 8-1](#)
- [Working with Configuration Masters, page 8-3](#)
- [Publishing Configurations to Web Security Appliances, page 8-13](#)
- [Viewing Web Security Appliance Status, page 8-22](#)

## Overview of Managing Web Security Appliances

AsyncOS for Security Management enables you to enforce uniform web security policies and custom URL categories across geographically distributed networks. You can edit and publish configurations for Web Security appliances directly from the GUI of your Security Management appliance.

The process for managing your Web Security appliances is as follows:

- 
- Step 1**    **Web Security appliances.** Upgrade to AsyncOS 7.1 for Web. See the *Cisco IronPort AsyncOS 7.0 for Web User Guide* or the *Cisco IronPort AsyncOS 7.1 for Web User Guide*.
- Step 2**    **Web Security appliances.** Configure networking, authorization, and security services. See the *Cisco IronPort AsyncOS 7.1 for Web User Guide*.
- Be sure to meet the configuration requirements in [Important Notes About Using Configuration Masters, page 8-3](#).

- Step 3 Web Security appliances.** Configure and test policies. See the *Cisco IronPort AsyncOS 7.1 for Web User Guide*.
- Step 4 (Optional) Web Security appliances.** When settings are all as you want them, download a configuration file from the Web Security appliance. (You can use this file to speed configuration of a Configuration Master in the Security Management appliance.) See the *Cisco IronPort AsyncOS 7.1 for Web User Guide*.
- For compatibility of configuration files and Configuration Master versions, see [Table 2-5\(Deployments with WSAs Only\) Configuration Master Compatibility, page 2-33](#).
- Step 5 Security Management appliance.** Enable the Cisco IronPort Centralized Configuration Manager. See [Enabling Services on the Security Management Appliance, page 3-2](#).
- Step 6 Security Management appliance.** Add the Web Security appliances to the Security Management appliance. See [Adding Managed Appliances, page 3-10](#).
- Step 7 Security Management appliance.** Edit the Security Services settings to match the state currently configured on your Web Security appliances. See [Editing Security Services Settings, page 8-3](#).
- Step 8 Security Management appliance.** Initialize the Configuration Masters. See [Initializing Configuration Masters, page 8-7](#).
- Step 9 Security Management appliance.** Associate Web Security appliances to the Configuration Masters. See [Associating Web Security Appliances to Configuration Masters, page 8-8](#).
- Step 10 Security Management appliance.** Import or manually configure policies, custom URL categories, and/or a web proxy bypass list in the Configuration Masters. See [Configuring Configuration Masters, page 8-9](#).
- Step 11 Security Management appliance.** Optionally, backup, restore, or upgrade your Security Management appliance. See [Backing Up Your Security Management Appliance, page 12-8](#).
- Step 12 Security Management appliance.** Publish configurations to your Web Security appliances. See [Publishing Configurations to Web Security Appliances, page 8-13](#).

# Working with Configuration Masters

You can use a Configuration Master to publish certain configurations (specifically, the settings under the Web Security Manager menu in the Web Security appliance) to Web Security appliances.

AsyncOS for Security Management provides multiple Configuration Masters, making it possible for you to centrally manage a heterogeneous deployment in which Web Security appliances run different versions of AsyncOS for Web Security containing different features.

Located within the Web section of the Security Management appliance GUI, each Configuration Master contains the configuration for a particular version of AsyncOS for Web Security.

For options for configuring your Configuration Masters, see [Configuring Configuration Masters, page 8-9](#).

## Important Notes About Using Configuration Masters

**Note**

If you have multiple Web Security appliances, check each Web Security appliance to ensure that all Realm Names in Network > Authentication are unique across appliances, unless the settings for same-name realms are identical.

**Note**

The Security Management appliance can publish a Configuration Master only to a Web Security appliance that is running a compatible version of AsyncOS (for example, if the Web Security appliance is running AsyncOS 6.3, then you assign it to Configuration Master 6.3). See [Adding Managed Appliances, page 3-10](#).

## Editing Security Services Settings

Before you begin using the Configuration Masters, edit the security services settings to customize the Configuration Master display to reflect the configuration of your Web Security appliances. These settings make the appropriate features available for configuration on the Security Management appliance.

By default, the **Web > Utilities > Security Services Display** page displays the settings for all Configuration Masters. “N/A” alongside a feature indicates that the feature is not available in that version of AsyncOS for Web Security.

You cannot use Configuration Masters to configure features not selected on the Security Services Display page, even if those features are enabled on your Web Security appliances.



### Warning

**To properly publish Configuration Master settings to managed Web Security appliances, the security services settings for the Configuration Master must match the settings on the Web Security appliances. Changing security services settings for a Configuration Master does not automatically change the settings on the Web Security appliances. Prior to publishing a Configuration Master, it is highly recommended that you check the Web > Utilities > Web Appliance Status page for mismatches between the security services settings and the settings on the Web Security appliances (see [Viewing Web Security Appliance Status, page 8-22](#)). If you note a mismatch, you must change either the security services settings (see [Editing Security Services Settings, page 8-3](#)) or the settings on the Web Security appliances.**

**Figure 8-1 Security Services Display Page**

### Security Services Display

| Configuration Master Settings for Display of Security Services |                       |                                   |                                                                             |
|----------------------------------------------------------------|-----------------------|-----------------------------------|-----------------------------------------------------------------------------|
| Features                                                       | Configuration Masters |                                   |                                                                             |
|                                                                | 5.7                   | 6.3                               | 7.1                                                                         |
| Transparent mode                                               | Yes                   | Yes                               | Yes                                                                         |
| FTP Proxy                                                      | N/A                   | Yes                               | Yes                                                                         |
| HTTPS Proxy                                                    | Yes                   | Yes                               | Yes                                                                         |
| Upstream Proxy Groups                                          | Yes                   | Yes                               | Yes                                                                         |
| Acceptable Use Controls                                        | IronPort URL Filters  | Cisco IronPort Web Usage Controls | Cisco IronPort Web Usage Controls (with Application Visibility and Control) |
| Mobile User Security                                           | N/A                   | N/A                               | IP Range                                                                    |
| Web Reputation Filters                                         | Yes                   | Yes                               | Yes                                                                         |
| Webroot Anti-Malware                                           | Yes                   | Yes                               | Yes                                                                         |
| McAfee Anti-Malware                                            | Yes                   | Yes                               | Yes                                                                         |
| Sophos Anti-Malware                                            | N/A                   | N/A                               | Yes                                                                         |
| End-User Acknowledgement                                       | Yes                   | Yes                               | Yes                                                                         |
| IronPort Data Security Filters                                 | N/A                   | Yes                               | Yes                                                                         |
| External DLP Servers                                           | N/A                   | Yes                               | Yes                                                                         |
| Credential Encryption                                          | N/A                   | N/A                               | No                                                                          |
| Identity Provider for SaaS                                     | N/A                   | N/A                               | Yes                                                                         |
| <a href="#">Edit Display Settings...</a>                       |                       |                                   |                                                                             |

To edit security services settings:

**Step 1** On the Security Management appliance, choose **Web > Utilities > Security Services Display**.

**Step 2** Click **Edit Settings**.

The Edit Security Services Display page appears and lists the features that appear in the Configuration Masters.



**Note** Web Proxy is not listed as a feature, because it is assumed that the Web Proxy is enabled in order to execute any of the managed policy types on the Web Security appliances. If the Web Proxy is disabled, any policies published to the Web Security appliances will be ignored.

**Step 3** (Optional) If you do not want to use one of the Configuration Masters, hide it by unchecking its corresponding Configuration Master check box on the **Edit Security Services Display** page.

| Management Appliance | Email     | Web                      |
|----------------------|-----------|--------------------------|
| Reporting            | Utilities | Configuration Master 7.1 |

### Edit Security Services Display

**Configuration Master Security Services Display Settings**

Please match the state currently configured on your Web Security Appliances. If there is variation within your deployment you should answer "yes" if the option is used on any appliance in your deployment.

☐ Configuration Master 5.7

Enable this Configuration Master to display the available options.

☐ Configuration Master 6.3

Enable this Configuration Master to display the available options.

☒ Configuration Master 7.1

| Web Appliance Options for Configuration Master 7.1                  | Yes                                                                                                                          |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Do your Web Appliances have <b>Transparent mode</b> enabled? ⓘ      | <input checked="" type="checkbox"/>                                                                                          |
| Do your Web Appliances have <b>FTP Proxy</b> enabled?               | <input checked="" type="checkbox"/>                                                                                          |
| Do your Web Appliances have <b>HTTP Proxy</b> enabled? ⓘ            | <input checked="" type="checkbox"/>                                                                                          |
| Are <b>Upstream Proxy Groups</b> configured on your appliances? ⓘ   | <input type="checkbox"/>                                                                                                     |
| Do your Web Appliances have <b>Acceptable Use Controls</b> enabled? | <div>Cisco IronPort Web Usage Controls ⓘ</div> <input checked="" type="checkbox"/> Enable Application Visibility and Control |
| Do your Web Appliances have <b>Mobile User Security</b> enabled?    | <div>Cisco ASA ⓘ</div> <input checked="" type="checkbox"/>                                                                   |
| Do your Web Appliances have <b>Web Reputation Filters</b> enabled?  | <input checked="" type="checkbox"/>                                                                                          |



**Note** When a Configuration Master is hidden, all references to it are removed from the GUI including the corresponding Configuration Master tab. Pending publish jobs that use the Configuration Master are deleted, and all Web Security appliances assigned to the hidden Configuration Master are re-categorized as not assigned. At least one Configuration Master must be enabled.

As an example, your **Security Services Display** page looks like the following where Configuration Master 5.7 and 6.3 are disabled:

Management Appliance | Email | Web

ReportingUtilitiesConfiguration Master 7.1

Security Services Display

Configuration Master Settings for Display of Security Services

|                                | Configuration Masters |                                   |                                                                             |
|--------------------------------|-----------------------|-----------------------------------|-----------------------------------------------------------------------------|
| Features                       | 5.7 (disabled)        | 6.3 (disabled)                    | 7.1                                                                         |
| Transparent mode               | Yes                   | Yes                               | Yes                                                                         |
| FTP Proxy                      | N/A                   | Yes                               | Yes                                                                         |
| HTTPS Proxy                    | Yes                   | Yes                               | Yes                                                                         |
| Upstream Proxy Groups          | Yes                   | No                                | No                                                                          |
| Acceptable Use Controls        | IronPort URL Filters  | Cisco IronPort Web Usage Controls | Cisco IronPort Web Usage Controls (with Application Visibility and Control) |
| Mobile User Security           | N/A                   | N/A                               | Cisco ASA                                                                   |
| Web Reputation Filters         | Yes                   | Yes                               | Yes                                                                         |
| Webroot Anti-Malware           | Yes                   | Yes                               | Yes                                                                         |
| McAfee Anti-Malware            | Yes                   | Yes                               | Yes                                                                         |
| Sophos Anti-Malware            | N/A                   | N/A                               | Yes                                                                         |
| End-User Acknowledgement       | Yes                   | Yes                               | Yes                                                                         |
| IronPort Data Security Filters | N/A                   | Yes                               | Yes                                                                         |
| External DLP Servers           | N/A                   | Yes                               | No                                                                          |
| Credential Encryption          | N/A                   | N/A                               | No                                                                          |
| Identity Provider for SaaS     | N/A                   | N/A                               | No                                                                          |
| Edit Display Settings          |                       |                                   |                                                                             |

**Step 4** Select or uncheck the **Yes** check box to reflect if the features are enabled on your Web Security appliances. If there is variation within your deployment, select the check box if the feature is enabled on *any* appliance in your deployment.

Features are as follows:

- Transparent Proxy Mode. If you use Forward mode, the proxy bypass feature will not be available.
- FTP Proxy. *Configuration Master 6.3 and 7.1 only.*
- HTTPS Proxy. HTTPS proxy must be enabled in order to configure decryption policies.
- Upstream Proxy Groups. Upstream proxy groups must be available on your Web Security appliances if you want to use routing policies.
- Acceptable Use Controls. Select the service that you want to use: Cisco IronPort URL Filters or Cisco IronPort Web Usage Controls.
- Web Reputation Filters.

- Webroot Anti-Malware.
  - McAfee Anti-Malware.
  - End User Acknowledgement.
  - Cisco IronPort Data Security Filters. *Configuration Master 6.3 and 7.1 only.*
  - External DLP Servers. *Configuration Master 6.3 and 7.1 only.*
- Step 5** Click **Submit**. The GUI displays specific warning messages if the changes you made to the security services settings will affect policies configured on your Web Security appliances. If you are sure that you want to submit your changes, click **Continue**.
- Step 6** On the **Security Services Display** page, confirm that **Yes** appears alongside each option that you selected.
- Step 7** Click **Submit** and then click **Commit** to commit your changes.
- 

## Initializing Configuration Masters

- Step 1** On the main Security Management appliance, choose **Web > Utilities > Configuration Masters**
- The Configuration Master page appears.
- Step 2** Click **Initialize** in the Options column.
- Step 3** On the Initialize Configuration Master page:
- If you have an existing Configuration Master for a previous release and you want to use or start with the same settings for the new Configuration Master, choose **Copy Configuration Master**.
- For compatibility of Configuration Master versions, see [Table 2-5\(Deployments with WSAs Only\) Configuration Master Compatibility, page 2-33](#).
- Otherwise, choose **Use default settings**.
- Step 4** Click **Initialize**.

The Configuration Master is now available.

## Associating Web Security Appliances to Configuration Masters

For each Web Security appliance that you want to centrally manage, the policy configuration must be associated to the Configuration Master that matches the appliance's AsyncOS version. For example, if the Web Security appliance is running AsyncOS 6.3 for Web, then it must be associated to Configuration Master 6.3. You can do this either while adding the Web Security appliances to the Security Management appliance (see [Adding Managed Appliances, page 3-10](#)) or through the **Web > Utilities > Configuration Masters** page.

There are three Configuration Masters available in this release: 5.7, 6.3, and 7.1.



### Note

Associating Web Security appliances to Configuration Masters does not automatically publish new configurations to the appliances. You must manually publish configurations to the appliances. See [Publishing Configurations to Web Security Appliances, page 8-13](#).

To associate appliances to a Configuration Master:

- Step 1** On the main Security Management appliance, choose **Web > Utilities > Configuration Masters**.  
The Configuration Master page appears.
- Step 2** Click **Edit Appliance Assignment List** to display the Configuration Master Assignments page.
- Step 3** In the rows of the appliances you want to associate, click to enter check marks in the **Masters** columns.



### Note

If a Configuration Master is hidden, the page does not display a column for that Configuration Master. To enable the hidden Configuration Master, navigate to **Web > Utilities > Security Services Display**. See [Editing Security Services Settings, page 8-3](#).



**Step 4** Click **Submit** and then click **Commit** to commit your changes.

**Note**

To view an example of how to upgrade or associate a Configuration Master to an appliance, see the [“Example 5: Upgrading to a New Configuration Master on an Existing Security Management Appliance”](#) section on page D-15.

## Configuring Configuration Masters

There are several ways to set up Configuration Masters:

- If you are upgrading from a previous release: Copy or import an earlier, existing Configuration Master into a new Configuration Master version.
- If you have already configured a Web Security appliance and want to use the same configurations for multiple Web Security appliances: Import a configuration file from an already-configured Web Security appliance.

See [Populating a Configuration Master with Existing Web Security Appliance Settings](#), page 8-10.

- If you have not yet configured policy settings, URL categories, or bypass settings on a Web Security appliance, set up an appropriate Configuration Master on the Security Management appliance.

For more information, see [About Configuring Web Security Features Using Configuration Masters](#), page 8-11.

**Note**

Changes that you make to a Configuration Master are not applied to the Web Security appliances assigned to the Configuration Master until after you have published the edited configuration. See [Publishing Configurations to Web Security Appliances](#), page 8-13.

## Populating a Configuration Master with Existing Web Security Appliance Settings

If you already have a working configuration that you want to use from one of your Web Security appliances, you can import the configuration file to the Security Management appliance to create default policy settings for a Configuration Master. The Configuration Master accepts configuration files from Web Security appliances of the same version.

For example, if you are loading an XML file into a Configuration Master, the file must be from the same version as the Configuration Master itself. That is, only files from a 6.3 machine can go into a 6.3 Configuration Master. Further, only files from a 7.1 machine can go into a 7.1 Configuration Master.

For compatibility of configuration files and Configuration Master versions, see [Table 2-5\(Deployments with WSAs Only\) Configuration Master Compatibility, page 2-33](#).



### Warning

**You can import compatible web configuration files as often as you want, even if you have already published configurations to your managed Web Security appliances. However, be aware that importing a configuration file to a Configuration Master completely overwrites the settings associated with the selected Configuration Master. In addition, the security services settings on the Security Services Display page are set to match the imported configuration.**

To populate the Configuration Master with a web configuration file:

- 
- Step 1** Save a configuration file from the Web Security appliance.
  - Step 2** On the main Security Management appliance, choose **Web > Utilities > Configuration Masters**.
  - Step 3** In the Options column, choose **Import Configuration**.  
The Import Web Configuration page appears. In this example Configuration Master 7.1 has been selected.
  - Step 4** From the Select Configuration drop-down list, select Web Configuration File.

**Figure 8-2 Import Web Configuration Page**

No Changes Pending

### Import Web Configuration for Configuration Master 7.1

Select Web Configuration

Select Configuration Source:

Web Configuration File

New Master Defaults:

The selected file will be used to create default policy settings for the selected Configuration Master. The selected configuration file must be compatible with the Configuration Master (7.1); typically, the Configuration Master will accept versions of the Web Security Appliance configuration file which are the same version or earlier than the configuration master version.

Load a valid configuration from a Web Security Appliance.

Browse...

- Step 5** In the New Master Defaults section, click **Browse** and select a valid configuration file from a Web Security appliance.
- Step 6** Click **Import File**.
- Step 7** Click **Import** to proceed with the import process, or click **Cancel**.

## About Configuring Web Security Features Using Configuration Masters

You can configure Web Security appliance features directly in the Security Management appliance GUI, and then publish the configuration changes to the Web Security appliances assigned to the Configuration Masters.

Located within the Web section of the Security Management appliance GUI, each Configuration Master contains the configuration for a particular version of AsyncOS for Web Security. This release of AsyncOS for Security Management contains Configuration Masters supporting AsyncOS 5.7 for Web Security, AsyncOS 6.3 for Web Security, and AsyncOS 7.1 for Web Security.

### Using Configuration Master 5.7

Configuration Master 5.7 enables you to configure identities, decryption policies, routing policies, access policies, and time-based policies; bypass the web proxy; and create custom URL categories.

Instructions for configuring these features in the Configuration Master are the same as instructions for configuring them on the Web Security appliance. See the *Cisco IronPort AsyncOS for Web User Guide*.

**Figure 8-3 Configuration Master 5.7**

| Management Appliance        |              |                             |  | Email                    | Web    |
|-----------------------------|--------------|-----------------------------|--|--------------------------|--------|
| Utilities                   |              | Configuration Master 5.7    |  | Configuration Master 6.3 |        |
| <b>Identities</b>           |              | <b>Web Security Manager</b> |  |                          |        |
|                             |              | Identities                  |  |                          |        |
|                             |              | Decryption Policies         |  |                          |        |
|                             |              | Routing Policies            |  |                          |        |
|                             |              | Access Policies             |  |                          |        |
| <b>Client / Transaction</b> |              |                             |  |                          |        |
| Add Identity...             |              |                             |  |                          |        |
| Order                       | Membership D | Custom URL Categories       |  | End-User Acknowledgement | Delete |
|                             | Global Ident | Time Ranges                 |  | Required                 |        |

Authentication: Enabled Disabled

## Using Configuration Master 6.3

Configuration Master 6.3 enables you to configure identities, decryption policies, routing policies, access policies, time-based policies, Cisco IronPort data security policies, and external DLP policies; bypass the web proxy; and create custom URL categories.

Instructions for configuring these features in the Configuration Master are the same as instructions for configuring them on the Web Security appliance. See the *Cisco IronPort AsyncOS for Web User Guide*.

**Figure 8-4 Configuration Master 6.3**

| Management Appliance                             |                        |                                 |  | Email                    | Web    |
|--------------------------------------------------|------------------------|---------------------------------|--|--------------------------|--------|
| Utilities                                        |                        | Configuration Master 5.7        |  | Configuration Master 6.3 |        |
| <b>Identities</b>                                |                        | <b>Web Security Manager</b>     |  |                          |        |
|                                                  |                        | Identities                      |  |                          |        |
|                                                  |                        | Decryption Policies             |  |                          |        |
|                                                  |                        | Routing Policies                |  |                          |        |
|                                                  |                        | Access Policies                 |  |                          |        |
| <b>Client / Transaction Identity Definitions</b> |                        |                                 |  |                          |        |
| Add Identity...                                  |                        |                                 |  |                          |        |
| Order                                            | Membership Definition  | Ironport Data Security Policies |  | End-User Acknowledgement | Delete |
|                                                  | Global Identity Policy | External DLP Policies           |  | Required                 |        |

Authentication: Enabled Disabled

Copyright © 2003-2009 IronPort Systems, Inc. All rights reserved.

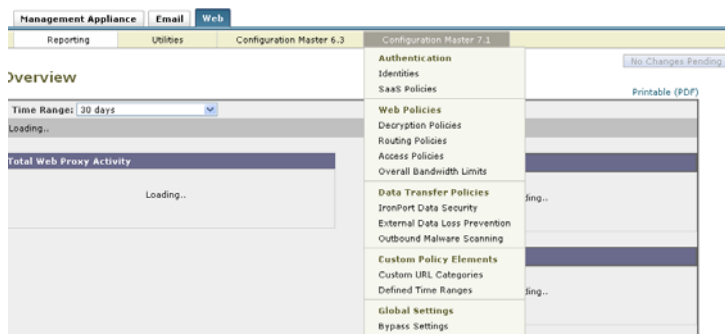
## Using Configuration Master 7.1

The Security Management appliance now supports Configuration Master 7.1. Configuration Master 7.1 enables you to configure authentication identities, SaaS policies, define web policies including decryption policies, routing policies,

access policies, defined time ranges, and overall bandwidth limits. Also included in this Configuration Master are the following: AVC, Sophos, credential encryption, Mobile User Security (MUS). You can also define Cisco IronPort data security policies, and external DLP policies; bypass the web proxy; and create custom URL categories including extended URL policies.

Instructions for configuring these features in the Configuration Master are the same as instructions for configuring them on the Web Security appliance. See the *Cisco IronPort AsyncOS for Web User Guide*.

**Figure 8-5 Configuration Master 7.1**



## Publishing Configurations to Web Security Appliances

AsyncOS for Security Management provides two types of configuration publishing. Although you initiate both types from the same pages in the Configuration Masters in the GUI, and you can perform both types as often as you want, each type yields very different results.

### Configuration Master Publish

After editing settings in a Configuration Master, you can publish them to the Web Security appliances associated to the Configuration Master.

You use Configuration Masters to edit the following Web Security appliance configuration variables only: policies (including access, decryption, SaaS, L4 Traffic Manager, routing and identities), proxy bypass lists, outbound malware scanning, time ranges, policy tags, URL tags, custom URL categories, FTP proxy (Configuration Master 6.3 and 7.1 only), Cisco IronPort Data Security Filters (Configuration Master 6.3 and 7.1 only), and external DLP servers (Configuration Master 6.3 and 7.1 only).

You will not be able to use the Configuration Masters to edit other configuration variables (for example: users, alerts, and log subscriptions).

You publish a Configuration Master to overwrite existing policy information on the Web Security appliances associated to that Configuration Master.



#### Note

---

Publishing External DLP policies from a Security Management appliance to multiple Web Security appliances that are not configured for RSA servers is not an issue. When you try to publish, the Security Management appliance, will send the following publish status warning, **“The Security Services display settings configured for Configuration Master 7.1 do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request. The affected appliances are: “[WSA Appliance Name]”. This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master. Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue. Do you want to continue publishing the configuration now?”**

If you decide to continue to publish, the Web Security appliance that is not configured for the RSA servers will receive the External DLP policies, but these policies will be disabled. The Web Security appliance External DLP page will not show the published policies if External DLP Server is not configured.

---

See [Publishing a Configuration Master, page 8-15](#). For more information about Configuration Masters, see [Working with Configuration Masters, page 8-3](#).

## Advanced File Publish

Advanced file publishing is completely independent of Configuration Master publishing and does not affect any of the configurations listed in the Configuration Master Publish section. Additionally, it will not affect

network/interface settings, DNS, SNTPD, WCCP, upstream proxy groups, certificates, the proxy mode, time settings, L4TM settings, authentication redirect hostname.

Use an advanced file publish to push a compatible XML configuration file from your local file system to managed Web Security appliances.

Advanced file publishing overrides non-policy configuration variables only (for example, users, alerts, and log subscriptions). You cannot use advanced file publishing to change policy information on managed Web Security appliances; in other words, if you can change a setting by publishing a Configuration Master, then you cannot change it by using an advanced file publish.

See [Using Advanced File Publishing, page 8-18](#).



#### Note

Neither publishing type affects network settings on Web Security appliances. You must configure network settings directly on your managed Web Security appliances. See the *Cisco IronPort AsyncOS for Web User Guide*.

## Publishing a Configuration Master



#### Note

An appliance running 6.3 can be assigned to the 5.7 Configuration Master. The versions do not need to be identical, but you cannot assign an appliance to a Configuration Master that is newer than the version on the appliance.



#### Warning

**To properly publish Configuration Master settings to managed Web Security appliances, the acceptable use controls for the Configuration Master must match the settings on the Web Security appliances. Changing these settings for a Configuration Master does not automatically change the settings on the Web Security appliances. Prior to publishing a Configuration Master, it is highly recommended that you check the Web > Utilities > Web Appliance Status page for mismatches between the acceptable use settings and the settings on the Web Security appliances (see [Viewing Web Security Appliance Status, page 8-22](#)). If those do not match then the publish will fail. All other mismatches will result in the disabling of those policies, the details of which can be found**

in the Publish History page. If you note a mismatch, you must change either the acceptable use control settings (see [Editing Security Services Settings, page 8-3](#)) or the settings on the Web Security appliances.

To publish a Configuration Master to Web Security appliances now:

**Step 1** On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.

**Step 2** Click **Publish Configuration Now**.

The Publish Configuration Now page appears.

**Figure 8-6 Publish Configuration Now Page**

#### Publish Configuration Now

| Settings for Publishing          |                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name:                        | <input checked="" type="radio"/> System-generated job name (example: admin.31_Mar_2009.20:44)<br><input type="radio"/> User-defined job name: <input type="text"/> |
| Start Time:                      | Now 31 Mar 2009 20:44 (GMT)                                                                                                                                        |
| Configuration Master to Publish: | Configuration Master 5.7.0 ▾                                                                                                                                       |
| Web Appliances: ?                | Options... ▾                                                                                                                                                       |

*Note: Publishing will take place immediately when the Publish button is clicked - it is not necessary to "commit" these changes.*

Cancel

Publish

**Step 3** “System-generated job name” is selected by default, or enter a user-defined job name (80 characters or fewer).

**Step 4** Select the Configuration Master to publish.

Alternatively, select “Advanced file options” if you want to perform an advanced file publish. See [Using Advanced File Publishing, page 8-18](#).

**Step 5** Select the Web Security appliances to which you want to publish the Configuration Master. Choose “All assigned appliances” to publish the configuration to all appliances assigned to the Configuration Master.

or

Choose “Select appliances in list” to display the list of appliances assigned to the Configuration Master. Select the appliances to which you want to publish the configuration.

**Step 6** Click **Publish**. The Publish in Progress page appears. Red progress bars and text indicate that an error occurred during publishing. If another job is currently publishing, then your request will be executed when the previous job is complete.



**Note**

Details of the job in progress also appear on the **Web > Utilities > Publish to Web Appliances** page. Click **Check Progress** to access the Publish in Progress page.

To publish the Configuration Master to Web Security appliances at a later time:

**Step 1** On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.

**Step 2** Click **Schedule a Job**.

The Schedule a Job page appears.

**Figure 8-7** *Schedule a Job Page*

**Schedule a Job**

| Settings for Publishing          |                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name:                        | <input checked="" type="radio"/> System-generated job name (example: admin_31_Mar_2009.20:46)<br><input type="radio"/> User-defined job name: <input type="text"/> |
| Start Time:                      | <div>MM/DD/YYYY</div> <div>HH:MM</div>                                                                                                                             |
| Configuration Master to Publish: | Configuration Master 5.7.0                                                                                                                                         |
| Web Appliances: ?                | Options...                                                                                                                                                         |

*Note: The Publish job will be created when the Submit button is clicked - it is not necessary to "commit" these changes.*

**Step 3** “System-generated job name” is selected by default, or enter a user-defined job name (80 characters or fewer).

**Step 4** Enter the date and time when you want to publish the Configuration Master.

**Step 5** Select the Configuration Master to publish.

Alternatively, select “Advanced file options” if you want to perform an advanced file publish. See [Using Advanced File Publishing, page 8-18](#).

**Step 6** Select the Web Security appliances to which you want to publish the Configuration Master. Choose “All assigned appliances” to publish the configuration to all appliances assigned to the Configuration Master.

or

Choose “Select appliances in list” to display the list of appliances assigned to the Configuration Master. Select the appliances to which you want to publish the configuration.

**Step 7** Click **Submit**.

**Step 8** View a list of scheduled jobs on the **Web > Utilities > Publish to Web Appliances** page. To edit a scheduled job, click the name of the job. To cancel a pending job, click the corresponding trash can icon and confirm that you want to delete the job.

---

## Using the publishconfig Command

The Security Management appliance provides you with the ability to publish changes a Configuration Master using the following CLI command:

**publishconfig config\_master** [--job\_name] [--host\_list | host\_ip]

where **config\_master** is either 5.7, 6.3, or 7.1. This keyword is required. The option *job\_name* is optional and will be generated if it is not specified.

The option *host\_list* is a list of host names or IP addresses for Web Security appliances to be published, and will be published to all hosts assigned to the Configuration Master if not specified. The option *host\_ip* can be multiple host IP addresses, each separated by a comma.

To verify that the **publishconfig** command was successful, check the **smad\_logs** file. You can also verify that the publish history was successful from the Security Management appliance GUI by choosing **Web > Utilities > Web Appliance Status**. From this page choose the web appliance that you want the publish history details. Additionally, you can go the Publish History page: **Web > Utilities > Publish > Publish History**.

## Using Advanced File Publishing

To perform an advanced file publish, you can choose one of the following:

- [Advanced File Publish: Publish Configuration Now, page 8-19](#)
- [Advanced File Publish: Publish Later, page 8-20](#)

## Advanced File Publish: Publish Configuration Now

To perform an Advanced File Publish: Publish Configuration Now, use the following steps:

**Step 1** On the main Security Management appliance window, choose **Web > Utilities > Publish to Web Appliances**.

**Step 2** Click **Publish Configuration Now**.

The Publish Configuration Now page appears.

**Figure 8-8** Publish Configuration Now Page

### Publish Configuration Now

| Settings for Publishing          |                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name:                        | <input checked="" type="radio"/> System-generated job name (example: admin.31_Mar_2009.20:44)<br><input type="radio"/> User-defined job name: <input type="text"/> |
| Start Time:                      | Now 31 Mar 2009 20:44 (GMT)                                                                                                                                        |
| Configuration Master to Publish: | Configuration Master 5.7.0 ▾                                                                                                                                       |
| Web Appliances: (?)              | Options... ▾                                                                                                                                                       |

*Note: Publishing will take place immediately when the Publish button is clicked - it is not necessary to "commit" these changes.*

Cancel

Publish

**Step 3** “System-generated job name” is selected by default, or enter a user-defined job name (80 characters or fewer).

**Step 4** Select **Advanced file options**.

**Step 5** Click **Browse** to select the file that you want to publish.

The Publish Configuration Now page appears.

**Figure 8-9** Publish Configuration Now Page

### Publish Configuration Now

| Settings for Publishing          |                                                                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name:                        | <input checked="" type="radio"/> System-generated job name (example: admin.31_Mar_2009.20:48)<br><input type="radio"/> User-defined job name: <input type="text"/>                                                                                                 |
| Start Time:                      | Now 31 Mar 2009 20:48 (GMT)                                                                                                                                                                                                                                        |
| Configuration Master to Publish: | Advanced file options: ▾<br>Select a file from the local computer: <input type="text"/> <input type="button" value="Browse..."/><br><i>The selected file must be a Web Appliance configuration file compatible with the appliances to which you are publishing</i> |
| Web Appliances: (?)              | Options... ▾                                                                                                                                                                                                                                                       |

*Note: Publishing will take place immediately when the Publish button is clicked - it is not necessary to "commit" these changes.*

Cancel

Publish

- Step 6** From the Web Appliances drop-down list, choose **Select appliances in list** or **All assigned to Master** and then select the appliances to which you want to publish the configuration file.
- Step 7** Click **Publish**.

### Advanced File Publish: Publish Later

To perform an Advanced File Publish: Publish Later, use the following steps:

- Step 1** On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.
- Step 2** Click **Schedule a Job**.
- The Schedule a Job page appears.

**Figure 8-10** *Schedule a Job Page*

#### Schedule a Job

| Settings for Publishing                          |                                                                                                                                                                    |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name:                                        | <input checked="" type="radio"/> System-generated job name (example: admin.31_Mar_2009.20:46)<br><input type="radio"/> User-defined job name: <input type="text"/> |
| Start Time:                                      | <input type="text"/> <input type="button" value="..."/> <input type="text"/><br><small>MM/DD/YYYY      HH:MM</small>                                               |
| Configuration Master to Publish:                 | Configuration Master 5.7.0 <input type="button" value="v"/>                                                                                                        |
| Web Appliances: <input type="button" value="i"/> | Options... <input type="button" value="v"/>                                                                                                                        |

*Note: The Publish job will be created when the Submit button is clicked - it is not necessary to "commit" these changes.*

- Step 3** **System-generated job name** is selected by default, or enter a user-defined job name (80 characters or fewer).
- Step 4** Enter the date and time when you want to publish the configuration.
- Step 5** Select **Advanced file options** and click **Browse** to select the file that you want to publish.

**Figure 8-11 Schedule a Job Page: Advanced File Options****Schedule a Job**

| Settings for Publishing          |                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Name:                        | <input checked="" type="radio"/> System-generated job name (example: admin.31_Mar_2009.20:50)<br><input type="radio"/> User-defined job name:                                                                                                 |
| Start Time:                      | <div>MM/DD/YYYY</div> <div>HH:MM</div>                                                                                                                                                                                                        |
| Configuration Master to Publish: | <div>Advanced file options...</div> <div>Select a file from the local computer:</div> <div>Browse...</div> <div>The selected file must be a Web Appliance configuration file compatible with the appliances to which you are publishing</div> |
| Web Appliances: ?                | Options...                                                                                                                                                                                                                                    |

Note: The Publish job will be created when the Submit button is clicked - it is not necessary to "commit" these changes.

- Step 6** From the Web Appliances drop-down list, choose **Select appliances in list** or **All assigned to Master** and then select the appliances to which you want to publish the configuration file.
- Step 7** Click **Publish**.

## Viewing Publish History

Viewing the publish history is useful for checking for errors that may have occurred during publishing.

To view publish history:

- Step 1** On the Security Management appliance, choose **Web > Utilities > Publish History**.

The Publish History page appears:

**Publish History**

| Most Recent Publish Jobs Attempted |                                |                      |                      |         |
|------------------------------------|--------------------------------|----------------------|----------------------|---------|
| Job Name                           | Completion Time ▼              | Configuration Master | Number of Appliances | Status  |
| admin.07_Apr_2010.21:40            | 07 Apr 2010 17:40 (GMT -04:00) | 7.1                  | 1                    | Success |

Copyright © 2003-2010 Cisco Systems, Inc. All rights reserved.

The Publish History page lists all of your most recent publish jobs attempted. Column information includes: Job Name, Job Completion Time, Configuration Master used (or name of the XML configuration file, if you performed an advanced file publish), Number of Appliances to which you published the job, and Status (Success or Failure).

To view additional details about a particular job, click the specific job name hypertext link in the Job Name column.

The Publish History: Job Details page appears.

**Publish History: Job Details**

| Job Details               |                                |         |     |
|---------------------------|--------------------------------|---------|-----|
| Job Name:                 | admin.07_Apr_2010.21:40        |         |     |
| Configuration Master:     | 7.1                            |         |     |
| Completion Time:          | 07 Apr 2010 17:40 (GMT -04:00) |         |     |
| Appliance Details for Job |                                |         |     |
| Appliance Name            | IP Address                     | Status  |     |
| vm-04                     | 10.92.152.90                   | Success | N/A |
| <a href="#">← Back</a>    |                                |         |     |

On the Publish History: Job Details page you can view additional details about a particular appliance in the job by clicking the appliance name; the **Web > Utilities > Web Appliance Status** page appears. You can also view status details about a particular appliance in the job, click the corresponding Details link to view the details on the Web Appliance Publish Details page.

# Viewing Web Security Appliance Status

AsyncOS provides two Web Security appliance status reports. One provides a high-level summary of the Web Security appliances connected to your Security Management appliance; the other provides a detailed view into the status of each connected Web Security appliance. Status information includes general information about the connected Web Security appliances, their published configuration, publish history, and so forth.



**Note**

Any web appliance that you add to the Security Management appliance will display an entry in the **Web > Utilities > Web Appliance Status** page. However, only machines with support for centralized management will have data available for display. The versions which support management are all versions of the Web

Security appliance since 5.7, with the exception of 6.0. Therefore, any appliance running 5.7, 6.3, or 7.1 will have data to display. The 6.0 version will display an error message stating that no information is available

To view the Web Security appliance status perform the following steps:

**Step 1** On the Security Management appliance, choose **Web > Utilities > Web Appliance Status**.

The Web Appliance Status page appears.

**Figure 8-12 Web Appliance Status Page**

|                      |           |                            |
|----------------------|-----------|----------------------------|
| Management Appliance | Email     | Web                        |
| Reporting            | Utilities | Configuration Master 5.7.0 |
|                      |           | Configuration Master 7.1   |

**Web Appliance Status**

 Attention Required. Click on the appliance name for details. Total Web Appliances: 3

| Web Appliances                                                                                     |              |                 |                              |          |               |                   |          |
|----------------------------------------------------------------------------------------------------|--------------|-----------------|------------------------------|----------|---------------|-------------------|----------|
| Appliance Name ▲                                                                                   | IP Address   | AsyncOS Version | Last Published Configuration |          |               | Security Services |          |
|                                                                                                    |              |                 | User                         | Job Name | Configuration | Enabled           | Disabled |
|  vm-03            | 10.92.152.89 | 6.3.0-604       |                              |          | (unpublished) | 8                 | 5        |
|  vmw078-was04.dev | 10.92.145.13 |                 |                              |          | (unpublished) |                   |          |
|  wsa-04           | 10.92.152.90 | 7.1.0-027       |                              |          | (unpublished) | 9                 | 6        |

The Web Appliance Status page displays a list of your connected Web Security appliances, including appliance name, IP address, AsyncOS version, last published configuration information (user, job name, and configuration version), number of security services enabled or disabled, and total number of connected appliances (up to 150). The warning icon indicates when attention is required for one of your connected appliances.



#### Note

It can take several minutes for the Web Appliance Status page to reflect recent configuration changes that occurred on the Web Security appliances. To refresh the data immediately, click the **Refresh Data** link. The time stamp on the page tells you when the data was last refreshed.

To view details about the status of a Web Security appliance:

**Step 1** On the Security Management appliance, choose **Web > Utilities > Web Appliance Status**.

**Step 2** Click the name of the appliance you want to view.

Details include:

- System status information (uptime, appliance model and serial number, AsyncOS version, build date, AsyncOS installation date and time, and host name)
- Configuration publish history (publish date/time, job name, configuration version, result of the publish, and user)
- Web Security features (feature description, configuration summary, security services settings, and status of feature keys)
- Proxy settings (upstream proxies and HTTP ports to proxy)
- Authentication service (name, protocol, and servers of authentication realms; name and order of realms in authentication sequences; and whether to block or permit traffic if authentication fails)

**Step 3** To refresh the details, if for example you have added new appliance, or if a message appears indicating that information for the appliance is not yet available, click the **Refresh Data** link. The time stamp on the page tells you when the data was last refreshed.

To find out more granular details about a specific Web Security appliance, click on the hypertext link in the Web Appliance column. The following page appears:





Figure 8-13 Web Appliance Status Details page

Appliance Status: vmw095-wsa11.sma (vmw095-wsa11.sma)

Data Refreshed: 06 Aug 2010 21:55 (GMT +03:00)

Refresh Data

| Appliance Status                                                                                                                                                    |                                       |                                |                       |                |              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|--------------------------------|-----------------------|----------------|--------------|
| System                                                                                                                                                              |                                       |                                |                       |                |              |
| Uptime:                                                                                                                                                             | 8 hours, 53 mins, 52 secs             |                                |                       |                |              |
| Up since:                                                                                                                                                           | 06 Aug 2010 13:01 (GMT +03:00)        |                                |                       |                |              |
| Model:                                                                                                                                                              | S10                                   |                                |                       |                |              |
| Serial Number:                                                                                                                                                      | 000C29EA7DC-vmware                    |                                |                       |                |              |
| AsyncOS Version:                                                                                                                                                    | 7.1.0-265 for Web                     |                                |                       |                |              |
| Build Date:                                                                                                                                                         | 2010-08-05                            |                                |                       |                |              |
| AsyncOS Install Date/Time:                                                                                                                                          | 2010-08-06 13:27:57                   |                                |                       |                |              |
| Configured Time Zone:                                                                                                                                               | Europe/Kiev                           |                                |                       |                |              |
| Host Name:                                                                                                                                                          | vmw095-wsa11.sma                      |                                |                       |                |              |
| Centralized Configuration Manager                                                                                                                                   |                                       |                                |                       |                |              |
| Configuration Publish History:                                                                                                                                      | Publish Date/Time                     | Job Name                       | Configuration Version | Result         | User         |
|                                                                                                                                                                     | <b>06 Aug 2010 14:56 (GMT +03:00)</b> | <b>admin.06_Aug_2010.14:55</b> | <b>7.1 (current)</b>  | <b>Success</b> | <b>admin</b> |
| The last successful configuration published appears in bold.<br>For a complete list of appliances in each publishing event, go to Web > Utilities > Publish History |                                       |                                |                       |                |              |
| Centralized Reporting                                                                                                                                               |                                       |                                |                       |                |              |
| Status:                                                                                                                                                             | Connected and transferred data        |                                |                       |                |              |
| Last Data Transfer Attempt:                                                                                                                                         | 06 Aug 2010 21:54 (GMT +03:00)        |                                |                       |                |              |

| Security Services                        |                       |                                               |        |                |                                       |
|------------------------------------------|-----------------------|-----------------------------------------------|--------|----------------|---------------------------------------|
| Description                              | Services              |                                               | Status | Time Remaining | Expiration Date                       |
|                                          | Web Appliance Service | Is Service Displayed on Management Appliance? |        |                |                                       |
| IronPort Web Proxy & DVS(TM) Engine      | Enabled               | N/A                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| IronPort L4 Traffic Monitor              | Enabled               | N/A                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| Proxy Mode                               | Transparent           | N/A                                           |        |                |                                       |
| FTP Proxy                                | Enabled               | Yes                                           |        |                |                                       |
| IronPort HTTPS Proxy                     | Enabled               | Yes                                           | Active | 29 days        | Sun 05 Sep 2010 13:14:45 (GMT +03:00) |
| Upstream Proxy Groups                    | Configured            | Yes (Routing Policies)                        |        |                |                                       |
| Mobile User Security                     | IP Range              | Yes (IP Range)                                | Active | 29 days        | Sun 05 Sep 2010 13:16:03 (GMT +03:00) |
| IronPort URL Filtering                   | Disabled              | N/A                                           | Active | 30 days        | Sun 05 Sep 2010 21:55:24 (GMT +03:00) |
| Cisco IronPort Web Usage Controls        | Enabled               | N/A                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| Application Visibility and Control       | Enabled               | N/A                                           |        |                |                                       |
| Cisco IronPort Centralized Web Reporting | Enabled               | N/A                                           |        |                |                                       |
| IronPort Web Reputation Filters          | Enabled               | Yes                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| Webroot Anti-Malware                     | Enabled               | Yes                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| McAfee Anti-Malware                      | Enabled               | Yes                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| Sophos Antivirus                         | Enabled               | Yes                                           | Active | 29 days        | Sun 05 Sep 2010 13:13:23 (GMT +03:00) |
| End-User Acknowledgement                 | Enabled               | Yes                                           |        |                |                                       |
| IronPort Data Security Filters           | Enabled               | Yes                                           |        |                |                                       |
| External DLP Servers                     | Configured            | Yes                                           |        |                |                                       |
| Credential Encryption                    | Disabled              | No                                            |        |                |                                       |
| Identity Provider for SaaS               | Configured            | Yes                                           |        |                |                                       |

| Acceptable Use Controls Engine Updates  |                       |                              |
|-----------------------------------------|-----------------------|------------------------------|
| Update Type                             | Web Appliance Version | Management Appliance Version |
| Web Categorization Categories List      | 1207964134            | 1207964134                   |
| Application Visibility and Control Data | 1278707745            | 1278707745                   |

| Mobile User Security Settings |  |
|-------------------------------|--|
| IP Range: 1.1.1.1-29          |  |

| Proxy Settings       |                                                    |
|----------------------|----------------------------------------------------|
| Upstream Proxies:    | Group: upstream_group<br>Proxies: 127.10.1.1:31261 |
| HTTP Ports to Proxy: | 80, 3128                                           |

| Authentication Service    |            |                                               |               |                           |  |
|---------------------------|------------|-----------------------------------------------|---------------|---------------------------|--|
| Authentication Realm:     | Name       | Protocol                                      | Servers       | Support Novell eDirectory |  |
|                           | sma19.sma  | LDAP                                          | sma19.sma:636 | Yes                       |  |
|                           | w2k3.qa    | NTLM                                          | w2k3.qa       | N/A                       |  |
|                           |            |                                               |               |                           |  |
|                           |            |                                               |               |                           |  |
| Authentication Sequences: | Name       | Order of Realms                               |               |                           |  |
|                           | sequences  | NTLMSSP: w2k3.qa<br>Basic: sma19.sma, w2k3.qa |               |                           |  |
|                           | All Realms | NTLMSSP: w2k3.qa<br>Basic: sma19.sma, w2k3.qa |               |                           |  |
|                           |            |                                               |               |                           |  |

**Note**

Warning messages will appear if different versions of the Acceptable Use Control Engine on the Web Security appliance do not match with those on the Security Management appliance. An 'N/A' is displayed if the service is disabled or not present on the Web Security appliance.



## CHAPTER 9

# Monitoring System Status

---

This chapter contains the following sections:

- [Monitoring Security Management Appliance Status, page 9-1](#)
- [Viewing the Status of Your Managed Appliances, page 9-8](#)
- [Monitoring Reporting Data Availability Status, page 9-9](#)
- [Monitoring Tracking Data Status, page 9-12](#)

## Monitoring Security Management Appliance Status

The System Status page is the first page that appears when you access the GUI of the Security Management appliance. For information about how to access the GUI, see [Accessing the Graphical User Interface, page 2-8](#).

To access the System Status page from anywhere in the GUI, select **Management Appliance > Centralized Services > System Status**.

Figure 9-1 System Status Page

## System Status

No Changes Pending

Printable (PDF)

| Centralized Services              |                                        |                                            |
|-----------------------------------|----------------------------------------|--------------------------------------------|
| Email Security                    |                                        |                                            |
| Spam Quarantine                   |                                        |                                            |
| Disk Quota Used: 0.0%             | Messages: 0                            | <i>Not enabled</i>                         |
| Centralized Reporting             |                                        |                                            |
| Processing Queue: 0.0%            | Status: Not enabled                    | <a href="#">Email Overview Report</a>      |
| Centralized Message Tracking      |                                        |                                            |
| Processing Queue: 0.0%            | Status: Not enabled                    | <a href="#">Track Messages</a>             |
| Web Security                      |                                        |                                            |
| Centralized Configuration Manager |                                        |                                            |
| Last Publish: N/A                 | Status: Never connected (2 Appliances) | <a href="#">View Appliance Status List</a> |
| Centralized Reporting             |                                        |                                            |
| Processing Queue: 0.0%            | Status: Never connected (2 Appliances) | <a href="#">Web Overview Report</a>        |

| Security Appliance Data Transfer Status |              |      |                   |                                   |
|-----------------------------------------|--------------|------|-------------------|-----------------------------------|
| Appliance                               |              |      | Connection Status |                                   |
| Name                                    | IP Address   | Type | Status ▲          | Services                          |
| wsa-04                                  | 10.92.152.90 | Web  | Never connected   | Centralized Configuration Manager |
| vm-03                                   | 10.92.152.89 | Web  | Never connected   | Centralized Configuration Manager |

| System Information                                                                                                   |                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Uptime                                                                                                               | Version Information                                                                                                                                              |
| Appliance Up Since: 22 Jan 2010 21:01 (GMT)<br>(3d 1h 40m 16s)                                                       | Model: M600<br>Operating System: 6.9.0-081<br>Build Date: 21 Jan 2010 00:00 (GMT)<br>Install Date: 22 Jan 2010 20:18 (GMT)<br>Serial Number: 000C29016FA8-vmware |
| CPU Utilization                                                                                                      | Hardware                                                                                                                                                         |
| Security Management Appliance: 0.0%<br>Quarantine Service: 0.0%<br>Reporting Service: 1.0%<br>Tracking Service: 0.0% | RAID Status: Unknown                                                                                                                                             |
| <b>Total CPU Utilization: 1.0%</b>                                                                                   |                                                                                                                                                                  |

Before you enable monitoring services and add a managed appliance, only the System Information section provides status information. If you have run the System Setup Wizard, enabled monitoring services, and added a managed appliance, the Services section and the Security Appliance Data Transfer Status section are populated with data. For information about enabling services, adding managed appliances, and viewing the status of both, see Chapter 3, 'Appliance Configuration,' on page 1, and [Viewing the Status of Your Managed Appliances](#), page 9-8.

## Centralized Services

The Centralized Services section provides an overview of services on the Security Management appliance.

On the main Security Management appliance, choose **Management Appliance > Centralized Services > System Status**, to view summary information about the transfer of reporting data between the managed Email Security appliances, Web Security appliances, and the Security Management appliance.

There are two sections under **Centralized Services > System Status**:

- [Email Security](#)
- [Web Security](#)

### Email Security

The Email Security section pertains to information for the Email Security appliances only. The Email Security section displays information for:

- **Spam Quarantine**—In this section, you can see the number of messages held in the Cisco IronPort Spam Quarantine and the percentage of the disk quota used by the quarantine. Click the Spam Quarantine View link to access the Spam Quarantine page. For more information about the Cisco IronPort Spam Quarantine, see Chapter 7, 'Managing the Cisco IronPort Spam Quarantine,' on page 1.
- **Centralized Reporting**—In this section you can see the Processing Queue information which shows the percentage of the processing queue that is used by reporting data.

The processing queue stores centralized reporting and tracking files as they await processing by the Security Management appliance. Normally, the Security Management appliance receives batches of reporting and tracking files for processing. The percentage of reporting or tracking files in the processing queue typically fluctuates as the files are transmitted from Email Security appliances and processed by the Security Management appliance. If the processing queue usage percentage remains consistently high over several hours or days, then the system is running at or beyond capacity. In that case, consider removing some of the managed appliances from the Security Management appliance, installing additional Security Management appliances, or both.

**Note**

The processing queue percentages gauge the number of files in the queue. They do not take file size into account. The percentages provide only a rough estimate of the Security Management appliance's processing load.

Click the Email Overview Report link to access the Overview interactive report page. For more information about the Overview report page, see [Email Reporting Overview Page](#), in [Chapter 4, "Using Centralized Email Reporting."](#)

- **Centralized Message Tracking**—In this section you can view summary information about the transfer of tracking data between the managed Email Security appliances and the Security Management appliance. The Processing Queue field shows what percentage of the processing queue is taken up by tracking data. Click the Track Messages link to access the Message Tracking query page. For more information about tracking messages, see Chapter 6, 'Tracking Email Messages,' on page 1.

## Web Security

The Web Security section pertains to information for the Web Security appliances only. The Web Security section displays information for:

- **Centralized Reporting**—In this section you can see the Processing Queue information which shows the percentage of the processing queue that is used by reporting data.

The processing queue stores centralized reporting and tracking files as they await processing by the Security Management appliance. Normally, the Security Management appliance receives batches of reporting and tracking files for processing. The percentage of reporting or tracking files in the processing queue typically fluctuates as the files are transmitted from Web Security appliances and processed by the Security Management appliance. If the processing queue usage percentage remains consistently high over several hours or days, then the system is running at or beyond capacity. In that case, consider removing some of the managed appliances from the Security Management appliance, installing additional Security Management appliances, or both.

**Note**

The processing queue percentages gauge the number of files in the queue. They do not take file size into account. The percentages provide only a rough estimate of the Security Management appliance's processing load.

Click the Web Overview Report link to access the Overview interactive report page. For more information about the Overview report page, see [Understanding the Web Reporting Pages](#), in [Chapter 5, "Using Centralized Web Reporting."](#)

- **Centralized Configuration Manager**—In this section you can view summary information about the last successful configuration update of a Web Security appliance. You can click the interactive link that takes you to the last successfully published update on your system. Click the View Appliance Status List to view the status of individual appliances on the Security Management appliance. For more information the status of appliances currently on your system, see [Viewing the Status of Your Managed Appliances](#), page 9-8.

## Security Appliance Data Transfer Status

To perform centralized management functions, the Security Management appliance relies on the successful transfer of data from the managed appliances to the Security Management appliance. The Security Appliance Data Transfer Status section provides status information about each appliance that is managed by the Security Management appliance.

By default, the Security Appliance Data Transfer Status section displays up to ten appliances. If the Security Management appliance manages more than ten appliances, you can use the Items Displayed menu to select the number of appliances to display.

**Note**

Summary information about data transfer status appears in the Services section at the top of the System Status page. The Security Appliance Data Transfer Status section provides appliance-specific data transfer status.

In the Security Appliance Data Transfer Status section, you can view connection status issues for specific appliances. For detailed information, click an appliance name to view the Data Transfer Status page for the appliance.

**Figure 9-2 Data Transfer Status: <Appliance\_Name> Page****Data Transfer Status: esa01**[Printable \(PDF\)](#)

| Security Appliance Data Transfer Status |                            |      |
|-----------------------------------------|----------------------------|------|
| Service                                 | Last Data Transfer Attempt |      |
|                                         | Status                     | Time |
| Configuration Manager                   | Not enabled                | N/A  |
| Reporting                               | Never connected            | N/A  |
| Tracking                                | Never connected            | N/A  |
| ISQ Safelist/Blocklist                  | Never connected            | N/A  |

The Data Transfer Status: *Appliance\_Name* page shows when the last data transfer occurred for each monitoring service.

The data transfer status for Email Security appliances can be one of the following values:

- **Not enabled:** The monitoring service is not enabled on the Email Security appliance.
- **Never connected:** The monitoring service is enabled on the Email Security appliance, but no connection has been established between the Email Security appliance and the Security Management appliance.
- **Waiting for data:** The Email Security appliance has connected to the Security Management appliance, which is waiting to receive data.
- **Connected and transferred data:** A connection was established between the Email Security appliance and the Security Management appliance, and data were successfully transferred.
- **File transfer failure:** A connection was established between the Email Security appliance and the Security Management appliance, but the data transfer failed.

The data transfer status for Web Security appliances can be one of the following values:

- **Not enabled:** The centralized configuration manager is not enabled for the Web Security appliance.
- **Never connected:** The centralized configuration manager is enabled for the Web Security appliance, but no connection has been established between the Web Security appliance and the Security Management appliance.
- **Waiting for data:** The Web Security appliance has connected to the Security Management appliance, which is waiting to receive data.



- **Connected and transferred data:** A connection was established between the Web Security appliance and the Security Management appliance, and data were successfully transferred.
- **Configuration push failure:** The Security Management appliance attempted to push a configuration file to the Web Security appliance, but the transfer failed.
- **Configuration push pending:** The Security Management appliance is in the process of pushing a configuration file to the Web Security appliance.
- **Configuration push success:** The Security Management appliance successfully pushed a configuration file to the Web Security appliance.

Data transfer issues can reflect temporary network problems or appliance configuration issues. The statuses of “Never connected” and “Waiting for data” are normal, transient statuses when you first add a managed appliance to the Security Management appliance. If the status does not eventually change to “Connected and transferred data,” then the data transfer status might indicate a configuration issue.

If the “File transfer failure” status appears for an appliance, monitor the appliance to determine if the failure was caused by a network issue or by a problem with the appliance configuration. If no network issues prevent data transfer and the status does not change to “Connected and transferred data,” then you might need to change the appliance configuration to enable data transfer.

## System Information

The System Information section of the System Status page provides information about the operating system and performance of the Security Management appliance. The Uptime field shows when the appliance was last started and how long it has been running. The Version Information area lists the model number, the version of AsyncOS, the build and install dates of the operating system, and the serial number of the appliance.



### Note

You may need to supply the appliance serial number to assist Cisco IronPort Customer Support with troubleshooting.

**Figure 9-3**      **System Information Section of the System Status Page**

| System Information             |                                          |
|--------------------------------|------------------------------------------|
| Uptime                         |                                          |
| Appliance Up Since:            | 13 May 2008 20:15 (GMT)<br>(21h 50m 19s) |
| CPU Utilization                |                                          |
| Security Management Appliance: | 0.4%                                     |
| Quarantine Service:            | 0.0%                                     |
| Reporting Service:             | 0.0%                                     |
| Tracking Service:              | 0.0%                                     |
| <b>Total CPU Utilization:</b>  | <b>0.4%</b>                              |
| Version Information            |                                          |
| Model:                         | M600                                     |
| Operating System:              | 6.4.0-104                                |
| Build Date:                    | 10 May 2008 00:00 (GMT)                  |
| Install Date:                  | 13 May 2008 20:16 (GMT)                  |
| Serial Number:                 | 000000000000-000000                      |

The CPU Utilization percentages indicate the portion of the Security Management appliance's CPU processing that is devoted to each of the monitoring services. The percentages show the amount of CPU currently used by the three major services. Other operations of the Security Management appliance are grouped under the general heading "Security Management appliance."

The CPU utilization percentages change constantly. Refresh the browser display to view the most recent data.

## Viewing the Status of Your Managed Appliances

The Security Appliances page provides information about the status of your managed appliances.

To access the Security Appliances page, perform the following:

On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.

**Figure 9-4 Security Appliances Page****Security Appliances**

| Centralized Service Status             |                           |  |  |  |  |
|----------------------------------------|---------------------------|--|--|--|--|
| Centralized Web Configuration Manager: | Enabled, using 0 licenses |  |  |  |  |
| Centralized Web Reporting:             | Enabled, using 2 licenses |  |  |  |  |
| Spam Quarantine:                       | Service disabled          |  |  |  |  |
| Centralized Email Reporting:           | Enabled, using 0 licenses |  |  |  |  |
| Centralized Email Message Tracking:    | Service disabled          |  |  |  |  |

| Security Appliances                    |              |                       |           |                         |        |
|----------------------------------------|--------------|-----------------------|-----------|-------------------------|--------|
| Email                                  |              |                       |           |                         |        |
| <a href="#">Add Email Appliance...</a> |              |                       |           |                         |        |
| No appliances have been added.         |              |                       |           |                         |        |
| Web                                    |              |                       |           |                         |        |
| <a href="#">Add Web Appliance...</a>   |              |                       |           |                         |        |
| Appliance Name ▲                       | IP Address   | Services              |           | Connection Established? | Delete |
|                                        |              | Configuration Manager | Reporting |                         |        |
| vm-04                                  | 10.92.152.90 | ✓                     | ✓         | Yes                     |        |
| wsa-03                                 | 10.92.152.89 | ✓                     | ✓         | No                      |        |

Key: ✓ Selected

The Centralized Service Status section shows which services are enabled and how many licenses you have used for each service. The Security Appliances section lists the appliances you have added. Check marks indicate the enabled services, and the Connection Established? column shows whether or not file transfer access is properly configured. You can also add or delete an appliance. For more information, see [Adding Managed Appliances, page 3-10](#).

## Monitoring Reporting Data Availability Status

The Security Management appliance enables you to monitor the availability of reporting data for a specified time period. See the appropriate section for your appliance:

- [Monitoring Data Availability on your Email Security Appliances, page 9-9](#)
- [Monitoring Data Availability on your Web Security Appliances, page 9-11](#)

## Monitoring Data Availability on your Email Security Appliances

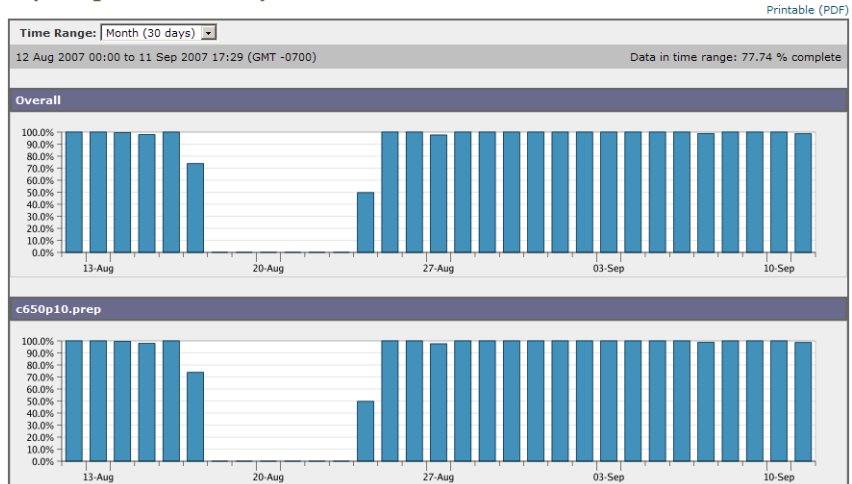
To monitor reporting data from your Email Security appliances on the Security Management appliance, perform the following:

**Step 1** On the Security Management appliance, choose **Email > Reporting > Reporting Data Availability**.

The Reporting Data Availability page appears.

**Figure 9-5** *Reporting Data Availability Page*

#### Reporting Data Availability



From the **Reporting Data Availability** page, you can view the percentage of reporting data that the Security Management appliance received from your Email Security appliances over a specified period of time. A bar chart indicates the completeness of the data received during the time range.

You can monitor reporting data availability for the preceding day, week, month, or year. If the Security Management appliance received less than 100% of the reporting data from the Email Security appliances, you can tell immediately that your data may be incomplete. Use the data availability information to validate reporting data and to troubleshoot system problems.



#### Note

If you have had to replace an Email Security appliance due to a hardware failure or other reasons, the data from the replaced Email Security appliance will not be lost, but the data will not be displayed correctly on the Security Management appliance.

# Monitoring Data Availability on your Web Security Appliances

To monitor reporting data from your Web Security appliances on the Security Management appliance, perform the following:

**Step 1** On the Security Management appliance, select **Web > Reporting > Data Availability**.

The Data Availability page appears.

From the Data Availability page you can update and sort data to provide real-time visibility into resource utilization and web traffic trouble spots.

## Web Reporting Data Availability

[Printable \(PDF\)](#)

| Web Reporting Data Range          |                                |                                |                                   |                                |                 |
|-----------------------------------|--------------------------------|--------------------------------|-----------------------------------|--------------------------------|-----------------|
| Displaying 1 - 2 of 2 appliances. |                                |                                |                                   |                                |                 |
| Web Security Appliance            | Web Reporting                  |                                | Web Tracking and Reporting Detail |                                | Status          |
|                                   | From ▼                         | To                             | From                              | To                             |                 |
| <a href="#">vmw098-wsa08.sma</a>  | 26 Aug 2010 09:00              | 27 Aug 2010 02:22              | 26 Aug 2010 11:00                 | 27 Aug 2010 02:22              | Ok              |
| <a href="#">vmw095-wsa11.sma</a>  | N/A                            | N/A                            | N/A                               | N/A                            | Never Connected |
| Overall:                          | 26 Aug 2010 09:00 (GMT +03:00) | 27 Aug 2010 02:22 (GMT +03:00) | 26 Aug 2010 11:00 (GMT +03:00)    | 27 Aug 2010 02:22 (GMT +03:00) |                 |
| Displaying 1 - 2 of 2 appliances. |                                |                                |                                   |                                |                 |



### Note

In the Web Reporting Data Availability window, Web Reporting will show disabled only if **both** Web Reporting and Email Reporting are disabled.

All data resource utilization and web traffic trouble spots are shown from this page. By clicking on one of the listed Web Security appliance links, you can view reporting data availability for that appliance.

You can monitor reporting data availability for the preceding day, week, month, or year. If the Security Management appliance received less than 100% of the reporting data from the Web Security appliances, you can tell immediately that your data may be incomplete. Use the data availability information to validate reporting data and to troubleshoot system problems.

If data availability is used within a scheduled report for URL Categories, and there are gaps in data for any of the appliances, the following message is displayed at the bottom of the page: “Some data in this time range was unavailable.” If there are no gaps present, nothing appears.

See the [“Data Availability Page”](#) for more information on the Data Availability page on the Web Security appliance.

## Monitoring Tracking Data Status

The Security Management appliance allows you to monitor and track data from any appliance.

- [Monitoring Email Tracking Data Status, page 9-12](#)
- [Monitoring Web Tracking Data Status, page 9-13](#)

## Monitoring Email Tracking Data Status



### Note

The Email Security appliance makes duplicate copies of reporting and tracking data taken from that appliance and places copies of the data files into additional folders apart from the default directory. The Security Management appliance can then be configured to pull data from one of those folders.

To monitor email tracking data status, perform the following:

- Step 1** On the main Security Management appliance, choose **Email > Message Tracking > Message Tracking Data Availability**.

The Message Tracking Data Availability page appears.

**Figure 9-6 Message Tracking Data Availability Page****Message Tracking Data Availability**[Printable \(PDF\)](#)

| Tracking Data Range |              |                               |                               |                            |
|---------------------|--------------|-------------------------------|-------------------------------|----------------------------|
| Security Appliance  |              | Data Range                    |                               | Status                     |
| IP Address          | Description  | From ▼                        | To                            |                            |
| 172.17.152.39       | c650p10.prep | 31 Jul 2007 01:40 (GMT -0700) | 11 Sep 2007 23:42 (GMT -0700) | Not updated in 438 minutes |
| Overall:            |              | 31 Jul 2007 01:40 (GMT -0700) | 11 Sep 2007 23:42 (GMT -0700) |                            |

| Missing Data Intervals |              |                               |                               |                        |
|------------------------|--------------|-------------------------------|-------------------------------|------------------------|
|                        |              | Items Displayed: 10           |                               | All Email Appliances ▼ |
| Security Appliance     |              | Missing Data Range            |                               |                        |
| IP Address             | Description  | From ▼                        | To                            |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 23:23 (GMT -0700) | 11 Sep 2007 23:41 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 23:03 (GMT -0700) | 11 Sep 2007 23:19 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 22:41 (GMT -0700) | 11 Sep 2007 22:59 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 22:19 (GMT -0700) | 11 Sep 2007 22:38 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 21:58 (GMT -0700) | 11 Sep 2007 22:16 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 21:37 (GMT -0700) | 11 Sep 2007 21:54 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 21:16 (GMT -0700) | 11 Sep 2007 21:33 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 20:59 (GMT -0700) | 11 Sep 2007 21:13 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 20:43 (GMT -0700) | 11 Sep 2007 20:56 (GMT -0700) |                        |
| 172.17.152.39          | c650p10.prep | 11 Sep 2007 20:21 (GMT -0700) | 11 Sep 2007 20:40 (GMT -0700) |                        |

The Message Tracking Data Availability page allows you to view the missing-data intervals for the Security Management appliance. A missing-data interval is a period of time during which the Security Management appliance received no message tracking data from your organization's Email Security appliances.

You can monitor data availability for a particular managed appliance or for all Email Security appliances in the system. If you find missing-data intervals in the message tracking data, you can immediately tell that your data may be incomplete. Use the data availability information to validate your message tracking data and to troubleshoot system problems.

## Monitoring Web Tracking Data Status

To monitor web tracking data status from the Security Management appliance, perform the following:

- Step 1** On the Security Management appliance, choose **Web > Reporting > Web Tracking**.

The Web Tracking Search dialog box appears

## Web Tracking

| Search                                                                |                              |
|-----------------------------------------------------------------------|------------------------------|
| Available: 31 Mar 2010 18:00 to 07 Apr 2010 19:59 (GMT -04:00)        |                              |
| Time Range:                                                           | Day                          |
| User/Client IP:                                                       | (e.g. jdoe or DOMAIN\jdoe)   |
| Website:                                                              | google.com (e.g. google.com) |
| Transaction Type:                                                     | All Transactions             |
| <a href="#">Advanced</a> Search transactions using advanced criteria. |                              |
| <a href="#">Clear</a>                                                 | <a href="#">Search</a>       |

- Step 2** From the Time Range drop-down list, select the time range that you want information about.
- Step 3** In the User/Client IP or the Website text field, enter a value.
- Step 4** From the Transaction Type drop-down list, select the type of transaction.
- Step 5** Choices include: All Transactions, Completed, Blocked, Monitored, Warned.
- The following example shows the results when 'google.com' is entered in the Website text field.

**Figure 9-7 Web Tracking Data Status Page**

Generated: 08 Apr 2010 16:57 (GMT -04:00) [Printable Download](#)

| Results              |                                                                                                                                                                                                                                                                                                                                                                                                          |                 |             |           |                  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------|-----------|------------------|
| Time (GMT -04:00)    | Transaction                                                                                                                                                                                                                                                                                                                                                                                              | Hide Details... | Disposition | Bandwidth | User / Client IP |
| 07 Apr 2010 17:44:14 | <a href="http://www.google-analytics.com/urchin.js">http://www.google-analytics.com/urchin.js</a><br>CONTENT TYPE: text/javascript URL CATEGORY: Software Updates<br>DESTINATION IP: 74.125.155.139 SERIAL: 000C29A511C8-vmware<br>DETAILS: DefaultGroup "Access". WBRs: -2.1.                                                                                                                           |                 | Allow       | 7,682B    | 173.37.10.190    |
| 07 Apr 2010 17:44:04 | <a href="http://www.google-analytics.com/_utm.gif?utmwv=4.6.5&amp;utmnn=1827679117&amp;utmhn=disq...">http://www.google-analytics.com/_utm.gif?utmwv=4.6.5&amp;utmnn=1827679117&amp;utmhn=disq...</a><br>CONTENT TYPE: image/gif URL CATEGORY: Search Engines and Portals<br>DESTINATION IP: 74.125.155.139 SERIAL: 000C29A511C8-vmware<br>DETAILS: DefaultGroup "Access". WBRs: -2.1.<br>PAGE ASSETS: 2 |                 | Allow       | 3,045B    | 173.37.10.190    |
| 07 Apr 2010 17:44:16 | <a href="http://www.open-opensocial.googleusercontent.com/gadgets/js/core:core.iourpc.js?...">http://www.open-opensocial.googleusercontent.com/gadgets/js/core:core.iourpc.js?...</a><br>CONTENT TYPE: text/javascript URL CATEGORY: Search Engines and Portals<br>DESTINATION IP: 74.125.155.132 SERIAL: 000C29A511C8-vmware<br>DETAILS: DefaultGroup "Access". WBRs: 5.9.                              |                 | Allow       | 18.5KB    | 173.37.10.190    |
| 07 Apr 2010 17:46:39 | <a href="http://safebrowsing.clients.google.com/safebrowsing/downloads?client=navclient-a-...">http://safebrowsing.clients.google.com/safebrowsing/downloads?client=navclient-a-...</a><br>CONTENT TYPE: text/plain URL CATEGORY: Search Engines and Portals<br>DESTINATION IP: 74.125.155.101 SERIAL: 000C29A511C8-vmware<br>DETAILS: DefaultGroup "Access". WBRs: 4.5.                                 |                 | Allow       | 1,696B    | 173.37.10.190    |
| 07 Apr 2010 17:46:40 | <a href="http://safebrowsing-cache.google.com/safebrowsing/r/d/Chfmb29uLXB0eXNoX2ZhdA...">http://safebrowsing-cache.google.com/safebrowsing/r/d/Chfmb29uLXB0eXNoX2ZhdA...</a><br>CONTENT TYPE: application/octet-stream URL CATEGORY: Search Engines and Portals<br>DESTINATION IP: 74.125.105.223 SERIAL: 000C29A511C8-vmware<br>DETAILS: DefaultGroup "Access". WBRs: 4.5.                             |                 | Allow       | 2,832B    | 173.37.10.190    |
|                      | PAGE ASSETS: 2                                                                                                                                                                                                                                                                                                                                                                                           |                 |             |           |                  |

For more information on Web Tracking, see the [Web Tracking Page, page 5-69](#).





# CHAPTER 10

## LDAP Queries

---

This chapter covers the following topics:

- [Overview, page 10-1](#)
- [Creating the LDAP Server Profile, page 10-3](#)
- [Configuring LDAP Queries, page 10-6](#)
- [Domain-Based Queries, page 10-12](#)
- [Chain Queries, page 10-14](#)
- [Configuring AsyncOS to Work With Multiple LDAP Servers, page 10-16](#)
- [Configuring External Authentication for Users, page 10-20](#)

## Overview

If you maintain end-user passwords and email aliases in a corporate LDAP directory — for example, in Microsoft Active Directory, SunONE Directory Server, or OpenLDAP directories — you can use the LDAP directory to authenticate users for access to the Cisco IronPort Spam Quarantine. When a user logs in to the web UI for the Cisco IronPort Spam Quarantine, the LDAP server validates the login name and password, and AsyncOS retrieves a list of the corresponding email aliases. Quarantined messages sent to any of the user's email aliases can appear in the Cisco IronPort Spam Quarantine, as long as the appliance does not rewrite them.

## Configuring LDAP to Work with the Cisco IronPort Spam Quarantine

When you configure your Cisco IronPort appliance to work with an LDAP directory, you must complete the following steps to set up for acceptance, routing, aliasing, and masquerading:

---

### Step 1 Configure an LDAP server profile.

The server profile contains information to enable AsyncOS to connect to the LDAP server, such as:

- Server name and port
- Base DN
- Authentication requirements for binding to the server

For more information about configuring a server profile, see [Creating the LDAP Server Profile, page 10-3](#).

When you create the LDAP server profile, you can configure AsyncOS to connect to multiple LDAP servers. For more information, see [Configuring AsyncOS to Work With Multiple LDAP Servers, page 10-16](#).

### Step 2 Configure the LDAP queries.

You can either use the default spam quarantine queries generated for the LDAP server profile or create your own queries that are tailored to your particular LDAP implementation and schema. You then designate the active queries for spam notifications and end-user access to the quarantine.

For information about queries, see [Configuring LDAP Queries, page 10-6](#).

### Step 3 Enable LDAP end-user access and spam notifications for the Cisco IronPort Spam Quarantine.

Enable LDAP end-user access to the Cisco IronPort Spam Quarantine to allow end-users to view and manage messages in their quarantine. You can also enable alias consolidation for spam notifications to prevent the user from receiving multiple notifications.

For more information, see [Configuring Cisco IronPort Spam Quarantine Settings, page 7-3](#).

---

# Creating the LDAP Server Profile

When you configure AsyncOS to use LDAP directories, you create an LDAP server profile to store the information about the LDAP server.

To create an LDAP server profile:

- Step 1** On the main Security Management appliance, choose **Management Appliance > System Administration > LDAP**.
- Step 2** Click **Add LDAP Server Profile**.

The Add LDAP Server Profile page is displayed.

**Figure 10-1** Configuring an LDAP Server Profile

## Add LDAP Server Profile

The screenshot shows the 'Add LDAP Server Profile' configuration page. The page is titled 'LDAP Server Settings' and contains several sections for configuring the LDAP server profile.

- Server Attributes**
  - LDAP Server Profile Name:** A text field for entering the profile name.
  - Host Name(s):** A text field for entering the host name(s). A note below the field states: 'Fully qualified hostname or IP, separate multiple entries with a comma'.
  - Authentication Method:** Two radio buttons: 'Anonymous' (selected) and 'Use Password'. If 'Use Password' is selected, there are text fields for 'Username:' and 'Password:'.
  - Server Type:** A dropdown menu with 'Unknown or Other' selected.
  - Port:** A text field with '3268' entered.
  - Base DN:** A text field for entering the base DN.
  - Connection Protocol:** A checkbox for 'Use SSL'.
  - Advanced:** A section containing:
    - Cache TTL (time-to-live):** A text field with '900' entered, followed by 'Seconds'.
    - Maximum Retained Cache Entries:** A text field with '10000' entered.
    - Maximum number of simultaneous connections for each host:** A text field with '10' entered.
    - Multiple host options:** Two radio buttons: 'Load-balance connections among all hosts listed' (selected) and 'Failover connections in the order listed'.
  - Server Attribute Testing:** A button labeled 'Test Server(s)'.
- External Authentication Queries**
  - ☐ External Authentication Queries
  - Not configured
- Spam Quarantine End-User Authentication Query**
  - ☐ Spam Quarantine End-User Authentication Query
  - Not configured
- Spam Quarantine Alias Consolidation Query**
  - ☐ Spam Quarantine Alias Consolidation Query

- Step 3** Enter a name for the server profile in the **LDAP Server Profile Name** text field.
- Step 4** Enter the host name for the LDAP server in the **Host Name(s)** text field.

You can enter multiple host names to configure the LDAP servers for failover or load-balancing. Separate multiple entries with commas. For more information, see [Configuring AsyncOS to Work With Multiple LDAP Servers, page 10-16](#).

- Step 5** Select an authentication method. You can use anonymous authentication or specify a username and password.



**Note** You need to configure LDAP authentication to view client user IDs instead of client IP addresses on reports. Without LDAP authentication the system can only refer to users by their IP address. Choose the **Use Password** radio button, and enter the User name and password. The user name will now be seen on the Internal Users Summary page.

- Step 6** Select the LDAP server type: Active Directory, OpenLDAP, or Unknown or Other.

- Step 7** Enter a port number.

The default port is 3268. This is the default port for Active Directory that enables it to access the global catalog in a multi-server environment.

- Step 8** Enter a base DN (distinguishing name) for the LDAP server.

If you authenticate with a username and a password, the username must include the full DN to the entry that contains the password. For example, a user with an email address of joe@example.com is a user of the marketing group. The entry for this user would look like the following entry:

```
uid=joe, ou=marketing, dc=example dc=com
```

- Step 9** Under Advanced, select whether to use SSL when communicating with the LDAP server.

- Step 10** Enter the cache time-to-live. This value represents the amount of time to retain caches.

- Step 11** Enter the maximum number of retained cache entries.

- Step 12** Enter a maximum number of simultaneous connections.

If you configure the LDAP server profile for load balancing, these connections are distributed among the listed LDAP servers. For example, if you configure 10 simultaneous connections and load balance the connections over three servers, AsyncOS creates 10 connections to each server, for a total of 30 connections. For more information, see [Load Balancing, page 10-19](#).




---

**Note** The maximum number of simultaneous connections includes LDAP connections used for LDAP queries. However, if you enable LDAP authentication for the Cisco IronPort Spam Quarantine, the appliance allows 20 additional connections for the end user quarantine for a total of 30 connections.

---

**Step 13** Test the connection to the server by clicking the **Test Server(s)** button. If you specified multiple LDAP servers, they are all tested. The results of the test appear in the Connection Status field. For more information, see [Testing LDAP Servers, page 10-6](#).

**Step 14** Create spam quarantine queries by selecting the check box and completing the fields.

You can configure the quarantine end-user authentication query to validate users when they log in to the end-user quarantine. You can configure the alias consolidation query so that end-users do not receive quarantine notices for each email alias. To use these queries, select the “Designate as the active query” check box. For more information, see [Configuring LDAP Queries, page 10-6](#).

**Step 15** Test the spam quarantine queries by clicking the **Test Query** button.

Enter the test parameters and click **Run Test**. The results of the test appear in the Connection Status field. If you make any changes to the query definition or attributes, click **Update**.




---

**Note** If you have configured the LDAP server to allow binds with empty passwords, the query can pass the test with an empty password field.

---

**Step 16** Click **Submit** and then click **Commit** to commit your changes.

Active Directory server configurations do not allow authentication through TLS with Windows 2000. This is a known issue with Active Directory. TLS authentication for Active Directory and Windows 2003 *does* work.




---

**Note** Although the number of server configurations is unlimited, you can configure only one end-user authentication query and one alias consolidation query per server.

---

## Testing LDAP Servers

Use the **Test Server(s)** button on the Add/Edit LDAP Server Profile page (or the `test` subcommand of the `ldapconfig` command in the CLI) to test the connection to the LDAP server. AsyncOS displays a message stating whether the connection to the server port succeeded or failed. If you configured multiple LDAP servers, AsyncOS tests each server and displays individual results.

## Configuring LDAP Queries

The following sections provide the default query strings and configuration details for each type of Cisco IronPort Spam Quarantine query:

- **Spam quarantine end-user authentication query.** For more information, see the [“Spam Quarantine End-User Authentication Queries”](#) section on page 10-8.
- **Spam quarantine alias consolidation query.** For more information, see [Spam Quarantine Alias Consolidation Queries](#), page 10-9.

To have the quarantine use an LDAP query for end-user access or spam notifications, select the “Designate as the active query” check box. You can designate one end-user authentication query to control quarantine access and one alias consolidation query for spam notifications. Any existing active queries are disabled. On the Security Management appliance, choose **Management Appliance > System Administration > LDAP** page, an asterisk (\*) is displayed next to the active queries.

You can also specify a domain-based query or chain query as an active end-user access or spam notification query. For more information, see [Domain-Based Queries](#), page 10-12 and [Chain Queries](#), page 10-14.



### Note

Use the **Test Query** button on the LDAP page (or the `ldaptest` command) to verify that your queries return the expected results.

## LDAP Query Syntax

Spaces are allowed in LDAP paths, and they do not need to be quoted. The CN and DC syntax is not case-sensitive.

Cn=First Last,oU=user,dc=domain,DC=COM

The variable names you enter for queries are case-sensitive and must match your LDAP implementation in order to work correctly. For example, entering **mailLocalAddress** at a prompt performs a different query than entering **maillocaladdress**.

## Tokens

You can use the following tokens in your LDAP queries:

- {a} username@domainname
- {d} domain
- {dn} distinguished name
- {g} group name
- {u} user name
- {f} MAILFROM: address



---

**Note**

The {f} token is valid in acceptance queries only.

---

For example, you might use the following query to accept mail for an Active Directory LDAP server: `(l(mail={a})(proxyAddresses=smtp:{a}))`



---

**Note**

We strongly recommend using the Test feature of the LDAP page (or the **test** subcommand of the **ldapconfig** command) to test all queries you construct and ensure that expected results are returned before you enable LDAP functionality on a listener. See the [“Testing LDAP Queries” section on page 10-11](#) for more information.

---

# Spam Quarantine End-User Authentication Queries

End-user authentication queries validate users when they log in to the Cisco IronPort Spam Quarantine. The token {u} specifies the user (it represents the user’s login name). The token {a} specifies the user’s email address. The LDAP query does not strip "SMTP:" from the email address; AsyncOS strips that portion of the address.

Based on the server type, AsyncOS uses one of the following default query strings for the end-user authentication query:

- **Active Directory:** (sAMAccountName={u})
- **OpenLDAP:** (uid={u})
- **Unknown or Other:** [Blank]

By default, the primary email attribute is **mail**. You can enter your own query and email attributes. To create the query in the CLI, use the `isqauth` subcommand of the `ldapconfig` command.



**Note**

If you want users to log in with their full email addresses, use (mail=smt~~p~~:{a}) for the query string.

## Sample Active Directory End-User Authentication Settings

This section shows sample settings for an Active Directory server and the end-user authentication query. This example uses password authentication for the Active Directory server, the default query string for end-user authentication for Active Directory servers, and the `mail` and `proxyAddresses` email attributes.

**Table 10-1**      *Example LDAP Server and Spam Quarantine End-User Authentication Settings: Active Directory*

|                       |                                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------|
| Authentication Method | Use Password<br>(Need to create a low-privilege user to bind for searching, or configure anonymous searching.) |
| Server Type           | Active Directory                                                                                               |
| Port                  | 3268                                                                                                           |
| Base DN               | [Blank]                                                                                                        |



**Table 10-1**      **Example LDAP Server and Spam Quarantine End-User Authentication Settings: Active Directory**

|                            |                      |
|----------------------------|----------------------|
| <b>Connection Protocol</b> | [Blank]              |
| <b>Query String</b>        | (sAMAccountName={u}) |
| <b>Email Attribute(s)</b>  | mail,proxyAddresses  |

## Sample OpenLDAP End-User Authentication Settings

This section shows sample settings for an OpenLDAP server and the end-user authentication query. This example uses anonymous authentication for the OpenLDAP server, the default query string for end-user authentication for OpenLDAP servers, and the `mail` and `mailLocalAddress` email attributes.

**Table 10-2**      **Example LDAP Server and Spam Quarantine End-User Authentication Settings: OpenLDAP**

|                              |                                                                   |
|------------------------------|-------------------------------------------------------------------|
| <b>Authentication Method</b> | <b>Anonymous</b>                                                  |
| <b>Server Type</b>           | OpenLDAP                                                          |
| <b>Port</b>                  | 389                                                               |
| <b>Base DN</b>               | [Blank] (Some older schemas will want to use a specific Base DN.) |
| <b>Connection Protocol</b>   | [Blank]                                                           |
| <b>Query String</b>          | (uid={u})                                                         |
| <b>Email Attribute(s)</b>    | mail,mailLocalAddress                                             |

## Spam Quarantine Alias Consolidation Queries

If you use spam notifications, the spam quarantine alias consolidation query consolidates the email aliases so that recipients do not receive quarantine notices for each alias. For example, a recipient might receive mail for the following email addresses: `john@example.com`, `jsmith@example.com`, and `john.smith@example.com`. When you use alias consolidation, the recipient receives a single spam notification at a chosen primary email address for messages sent to all of the user's aliases.

To consolidate messages to a primary email address, create a query to search for a recipient’s alternate email aliases, and then enter the attribute for the recipient’s primary email address in the Email Attribute field.

For Active Directory servers, the default query string is `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))` and the default email attribute is `mail`. For OpenLDAP servers, the default query string is `(mail={a})` and the default email attribute is `mail`. You can define your own query and email attributes, including multiple attributes separated by commas. If you enter more than one email attribute, Cisco IronPort recommends entering a unique attribute that uses a single value, such as `mail`, as the first email attribute instead of an attribute with multiple values that can change, such as `proxyAddresses`.

To create the query in the CLI, use the `isqalias` subcommand of the `ldapconfig` command.

Sample Active Directory Alias Consolidation Settings

This section shows sample settings for an Active Directory server and the alias consolidation query. This example uses anonymous authentication for the Active Directory server, a query string for alias consolidation for Active Directory servers, and the `mail` email attribute.

Table 10-3 Example LDAP Server and Spam Quarantine Alias Consolidation Settings: Active Directory

|                       |                                          |
|-----------------------|------------------------------------------|
| Authentication Method | Anonymous                                |
| Server Type           | Active Directory                         |
| Port                  | 3268                                     |
| Base DN               | [Blank]                                  |
| Connection Protocol   | Use SSL                                  |
| Query String          | <code>((mail={a})(mail=smtp:{a}))</code> |
| Email Attribute       | <code>mail</code>                        |

## Sample OpenLDAP Alias Consolidation Settings

This section shows sample settings for an OpenLDAP server and the alias consolidation query. This example uses anonymous authentication for the OpenLDAP server, a query string for alias consolidation for OpenLDAP servers, and the `mail` email attribute.

**Table 10-4**      **Example LDAP Server and Spam Quarantine Alias Consolidation Settings: OpenLDAP**

|                       |                                                                   |
|-----------------------|-------------------------------------------------------------------|
| Authentication Method | Anonymous                                                         |
| Server Type           | OpenLDAP                                                          |
| Port                  | 389                                                               |
| Base DN               | [Blank] (Some older schemas will want to use a specific Base DN.) |
| Connection Protocol   | Use SSL                                                           |
| Query String          | <code>(mail={a}))</code>                                          |
| Email Attribute       | <code>mail</code>                                                 |

## Testing LDAP Queries

Use the **Test Query** button on the Add/Edit LDAP Server Profile page (or the `ldaptest` command in the CLI) to test your queries. AsyncOS displays details about each stage of the query connection test. For example, whether the first stage SMTP authorization succeeded or failed, and whether the BIND match returned a true or false result.

The `ldaptest` command is available as a batch command, for example:

```
ldaptest LDAP.isqalias foo@cisco.com
```

The variable names you enter for queries are *case-sensitive* and must match your LDAP implementation to work correctly. For example, entering `mailLocalAddress` for the email attribute performs a different query than entering `maillocaladdress`.

To test a query, you must enter the test parameters and click **Run Test**. The results appear in the Test Connection field. If an end-user authentication query succeeds, a result of “Success: Action: match positive” is displayed. For alias consolidation queries, a result of “Success: Action: alias consolidation” is displayed, along with

the email address for the consolidated spam notifications. If a query fails, AsyncOS displays a reason for the failure, such as no matching LDAP records were found, or the matching record did not contain the email attribute. If you use multiple LDAP servers, the Cisco IronPort appliance tests the query on each LDAP server.

## Domain-Based Queries

Domain-based queries are LDAP queries that are grouped by type and associated with a domain. You might want to use domain-based queries if different LDAP servers are associated with different domains, but you need to run queries for all your LDAP servers for end-user quarantine access. For example, a company called Bigfish owns the domains Bigfish.com, Redfish.com, and Bluefish.com, and it maintains a different LDAP server for employees associated with each domain. Bigfish can use a domain-based query to authenticate end-users against the LDAP directories of all three domains.

To use a domain-based query to control end-user access or notifications for the Cisco IronPort Spam Quarantine, complete the following steps:

- 
- Step 1** Create an LDAP server profile for each domain you want to use in the domain-based query. In each server profile, configure the queries you want to use in the domain-based query. For more information, see [Creating the LDAP Server Profile, page 10-3](#).
  - Step 2** Create the domain-based query. When you create the domain-based query, you select queries from each server profile, and designate the domain-based query as an active query for the Cisco IronPort Spam Quarantine. For more information about creating the query, see [Creating a Domain-Based Query, page 10-13](#).
  - Step 3** Enable end-user access or spam notifications for the Cisco IronPort Spam Quarantine. For more information, see [Configuring Cisco IronPort Spam Quarantine Settings, page 7-3](#).
-

## Creating a Domain-Based Query

To create a domain-based query on the Security Management appliance, perform the following:

**Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > LDAP**.

**Step 2** On the LDAP page, click **Advanced**.

The Add Domain Assignments Page appears.

**Figure 10-2** *Configuring a Domain-Based Query*

### Add Domain Assignments

| Domain Assignments                                                                                                      |                                     |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Name: <input type="text" value="Bigfish_Auth"/>                                                                         |                                     |
| Query Type: <span>Spam Quarantine End-User Authentication</span> <input type="checkbox"/> Designate as the active query |                                     |
| Domain or Partial Domain                                                                                                | Query                               |
| <input type="text" value="bluefish.com"/>                                                                               | <span>Bluefish.isq_user_auth</span> |
| <input type="text" value="redfish.com"/>                                                                                | <span>Redfish.isq_user_auth</span>  |
| <a href="#">Add Row</a>                                                                                                 |                                     |
| Default Query: <span>None</span>                                                                                        |                                     |
| Test: <a href="#">Test Query</a>                                                                                        |                                     |

**Step 3** Enter a name for the domain-based query.

**Step 4** Select the query type.



**Note** When you create a domain-based query, you specify a single query type. After you select a query type, the query field drop-down lists contain the appropriate queries from the LDAP server profiles.

**Step 5** In the Domain Assignments field, enter a domain.

**Step 6** Select a query to associate with the domain.

**Step 7** Add a row and select a query for each domain in the domain-based query.

**Step 8** Enter a default query to run if all other queries fail. If you do not want to enter a default query, select **None**.

- Step 9** Test the query by clicking the **Test Query** button and entering a user login and password or an email address to test in the Test Parameters fields. The results appear in the Connection Status field.
- Step 10** Check the **Designate as the active query** checkbox if you want the Cisco IronPort Spam Quarantine to use the domain-based query.



**Note** The domain-based query becomes the active LDAP query for the specified query type. For example, if the domain-based query is used for end-user authentication, it becomes the active end-user authentication query for the Cisco IronPort Spam Quarantine.

- Step 11** Click **Submit** and then click **Commit** to commit your changes.



**Note** To do the same configuration on the command line interface, type the `advanced` subcommand of the `ldapconfig` command at the command line prompt.

## Chain Queries

A chain query is a series of LDAP queries that AsyncOS runs in succession. AsyncOS runs each query in the series each query in the “chain” until the LDAP server returns a positive response or the final query returns a negative response or fails. Chain queries can be useful if entries in LDAP directories use different attributes to store similar (or the same) values. For example, departments in an organization might use different types of LDAP directories. The IT department might use OpenLDAP while the Sales department uses Active Directory. To ensure that queries run against both types of LDAP directories, you can use chain queries.

To use a chain query to control end-user access or notifications for the Cisco IronPort Spam Quarantine, complete the following steps:

- Step 1** Create an LDAP server profile for each query you want to use in the chain queries. For each of the server profiles, configure the queries you want to use for a chain query. For more information, see [Creating the LDAP Server Profile, page 10-3](#).

- Step 2** Create the chain query and designate it as an active query for the Cisco IronPort Spam Quarantine. For more information, see [Creating a Chain Query, page 10-15](#).
- Step 3** Enable LDAP end-user access or spam notifications for the Cisco IronPort Spam Quarantine. For more information about the spam quarantine, see [Configuring Cisco IronPort Spam Quarantine Settings, page 7-3](#).

## Creating a Chain Query

To create a chain query, perform the following:

(or the `advanced` subcommand of the `ldapconfig` command in the CLI).

- Step 1** On the Security Management appliance, choose Management Appliance > System Administration > LDAP > LDAP Server.

- Step 1** From the LDAP Server Profiles page, click **Advanced**.

- Step 2** Click **Add Chained Query**.

The Add Chained Query page is displayed.

**Figure 10-3** *Configuring a Chain Query*

### Add Chained Query

| Chained Query     |                                                                                                |                       |
|-------------------|------------------------------------------------------------------------------------------------|-----------------------|
| Name:             | Chain_Query                                                                                    |                       |
| Query Type:       | Spam Quarantine End-User Authentication <input type="checkbox"/> Designate as the active query |                       |
| Order of Queries: | Order                                                                                          | Query                 |
|                   | 1                                                                                              | Server1.isq_user_auth |
|                   | 2                                                                                              | Server2.isq_user_auth |
| Test:             |                                                                                                | Test Query            |

- Step 3** Enter a name for the chain query.

- Step 4** Select the query type.

When you create a chain query, all of its component queries have the same query type. After you select a query type, the query field drop-down lists display the appropriate queries from the LDAP.

**Step 5** Select the first query in the chain.

The Cisco IronPort appliance runs the queries in the order you configure them. If you add multiple queries to the chain query, you might want to order them so that general queries follow granular queries.

**Step 6** Test the query by clicking the **Test Query** button and entering a user login and password or an email address in the Test Parameters fields. The results appear in the Connection Status field.

**Step 7** Check the **Designate as the active query** check box if you want the Cisco IronPort Spam Quarantine to use the domain query.



**Note** The chain query becomes the active LDAP query for the specified query type. For example, if the chain query is used for end-user authentication, it becomes the active end-user authentication query for the Cisco IronPort Spam Quarantine.

**Step 8** Click **Submit** and then click **Commit** to commit your changes.



**Note** To do the same configuration on the command line interface, type the `advanced` subcommand of the `ldapconfig` command at the command line prompt.

## Configuring AsyncOS to Work With Multiple LDAP Servers

When you configure an LDAP server profile, you can configure the Cisco IronPort appliance to connect to a list of multiple LDAP servers. If you use multiple LDAP servers, they need to contain the same information, have the same structure, and use the same authentication information. Third-party products exist that can consolidate the records.

You configure the Cisco IronPort appliance to connect to redundant LDAP servers to use the following features:



- **Failover.** If the Cisco IronPort appliance cannot connect to an LDAP server, it connects to the next server in the list.
- **Load Balancing.** The Cisco IronPort appliance distributes connections across the list of LDAP servers when it performs LDAP queries.

You can configure redundant LDAP servers on the Management Appliance > System Administration > LDAP page or by using the CLI `ldapconfig` command.

## Testing Servers and Queries

Use the **Test Server(s)** button on the Add (or Edit) LDAP Server Profile page (or the `test` subcommand in the CLI) to test the connection to an LDAP server. If you use multiple LDAP servers, AsyncOS tests each server and displays individual results for each server. AsyncOS will also test the query on each LDAP server and display the individual results.

## Failover

To ensure an LDAP server is available to that resolve queries, you can configure the LDAP profile for failover.

The Cisco IronPort appliance attempts to connect to the first server in the list of LDAP servers for a specified period of time. If the appliance cannot connect to the first LDAP server in the list, the appliance attempts to connect to the next LDAP server in the list. To ensure that the Cisco IronPort appliance connects to the primary LDAP server by default, enter it as the first server in the list of LDAP servers.

If the Cisco IronPort appliance connects to a second or subsequent LDAP server, it remains connected to that server for a specified period of time. At the end of this period, the appliance attempts to reconnect to the first server in the list.

## Configuring the Cisco IronPort Appliance for LDAP Failover

To configure the Cisco IronPort appliance for LDAP failover, perform the following:

**Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > LDAP**.

The LDAP Server Setup page appears.

| LDAP Server Settings      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Attributes         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LDAP Server Profile Name: | example.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Host Name(s):             | ldapsrv1.example.com, ldapsrv2.example.com, ldapsrv3.example.com<br><small>Fully qualified hostname or IP, separate multiple entries with a comma</small>                                                                                                                                                                                                                                                                                                                                                                                                           |
| Authentication Method:    | <input checked="" type="radio"/> Anonymous<br><input type="radio"/> Use Password<br>Username: <input type="text"/><br>Password: <input type="password"/>                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server Type: (?)          | Unknown or Other <input checked="" type="checkbox"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Port: (?)                 | 3268                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Base DN: (?)              | dc=example, dc=com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Advanced:                 | <div> <div>Connection Protocol:</div> <div><input type="checkbox"/> Use SSL</div> </div> <div> <div>Cache TTL (time-to-live):</div> <div>900 Seconds</div> </div> <div> <div>Maximum Retained Cache Entries:</div> <div>10000</div> </div> <div> <div>Maximum number of simultaneous connections for each host:</div> <div>10</div> </div> <div> <div>Multiple host options:</div> <div> <input type="radio"/> Load-balance connections among all hosts listed<br/> <input checked="" type="radio"/> Failover connections in the order listed         </div> </div> |

**Step 2** Select the LDAP server profile you want to edit.

In this example, the LDAP server name is example.com.

**Step 3** In the Hostname text field, type the LDAP Servers; for example **ldapsrv1.example.com**.

**Step 4** In the Maximum number of simultaneous connections for each host text field, type the maximum number of connections.

In this example the maximum number of connections is **10**.

**Step 5** Click on the radio button next to **Failover connections in the order list**.

**Step 6** Configure other LDAP options as necessary.

**Step 7** Click **Submit** and then click **Commit** to commit the changes.

## Load Balancing

To distribute LDAP connections among a group of LDAP servers, you can configure your LDAP profile for load balancing.

When you use load balancing, the Cisco IronPort appliance distributes connections among the LDAP servers listed. If a connection fails or times out, the Cisco IronPort appliance determines which LDAP servers are available and reconnects to available servers. The Cisco IronPort appliance determines the number of simultaneous connections to establish based on the maximum number of connections you configure.

If one of the listed LDAP servers does not respond, the Cisco IronPort appliance distributes the connection load among the remaining LDAP servers.

## Configuring the Cisco IronPort Appliance for Load Balancing

To configure the Cisco IronPort appliance for LDAP load balancing, perform the following:

- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > LDAP**.

The LDAP Server Setup page appears.

| LDAP Server Settings      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Attributes         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| LDAP Server Profile Name: | example.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Host Name(s):             | ldapsrv1.example.com, ldapsrv2.example.com, ldapsrv3.example.com<br><i>Fully qualified hostname or IP, separate multiple entries with a comma</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Authentication Method:    | <input checked="" type="radio"/> Anonymous<br><input type="radio"/> Use Password<br>Username: <input type="text"/><br>Password: <input type="password"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server Type: ?            | Unknown or Other <input type="button" value="v"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Port: ?                   | 3268                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Base DN: ?                | dc=example, dc=com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Advanced:                 | <div>           Connection Protocol: <input type="checkbox"/> Use SSL         </div> <div>           Cache TTL (time-to-live): <input type="text" value="900"/> Seconds         </div> <div>           Maximum Retained Cache Entries: <input type="text" value="10000"/> </div> <div>           Maximum number of simultaneous connections for each host: <input type="text" value="10"/> </div> <div>           Multiple host options:           <div> <input checked="" type="radio"/> Load-balance connections among all hosts listed             <input type="radio"/> Failover connections in the order listed           </div> </div> |

- Step 2** Select the LDAP server profile you want to edit  
In this example, the LDAP server name is `example.com`.
- Step 3** In the Hostname text field, type the LDAP Servers; for example **ldapservers.example.com**.
- Step 4** In the Maximum number of simultaneous connections for each host text field, type the maximum number of connections.  
In this example the maximum number of connections is **10**.
- Step 5** Click on the radio button next to **Load balance connections among all hosts**.
- Step 6** Configure other LDAP options as necessary.
- Step 7** Click **Submit** and then click **Commit** to commit the changes.
- 

## Configuring External Authentication for Users

You can configure the Cisco IronPort appliance to use an LDAP directory on your network to authenticate users by allowing them to log in with their LDAP usernames and passwords. After you configure the authentication queries for the LDAP server, enable the appliance to use external authentication on the **Management Appliance > System Administration > Users** page in the GUI (or use the `userconfig` command in the CLI).

To configure external authentication for users, complete the following steps:

- 
- Step 1** **Create a query to find user accounts.** In an LDAP server profile, create a query to search for user accounts in the LDAP directory.
- Step 2** **Create group membership queries.** Create a query to determine if a user is a member of a directory group, and create a separate query to find all members of a group.
- Step 3** **Set up external authentication to use the LDAP server.** Enable the appliance to use the LDAP server for user authentication and assign user roles to the groups in the LDAP directory. For more information, see “Adding Users” in the *Cisco IronPort AsyncOS for Email User Guide*.

**Note**

Use the Test Query button on the LDAP page (or the `ldaptest` command) to verify that your queries return the expected results. For more information, see [Testing LDAP Queries, page 10-11](#).

## User Accounts Query

To authenticate external users, AsyncOS uses a query to search for the user record in the LDAP directory and the attribute that contains the user's full name. Depending on the server type you select, AsyncOS enters a default query and a default attribute. You can choose to have your appliance deny users with expired accounts if you have attributes defined in RFC 2307 in your LDAP user records (**shadowLastChange**, **shadowMax**, and **shadowExpire**). The base DN is required for the domain level where user records reside.

[Table 10-5](#) shows the default query string and full username attribute that AsyncOS uses when it searches for a user account on an Active Directory server.

**Table 10-5**      **Default Query String for Active Directory Server**

| Server Type                               | Active Directory                                                       |
|-------------------------------------------|------------------------------------------------------------------------|
| Base DN                                   | [blank] (You need to use a specific base DN to find the user records.) |
| Query String                              | <code>(&amp;(objectClass=user)(sAMAccountName={u}))</code>             |
| Attribute containing the user's full name | <code>displayName</code>                                               |

[Table 10-6](#) shows the default query string and full username attribute that AsyncOS uses when it searches for a user account on an OpenLDAP server.

**Table 10-6**      **Default Query String for Open LDAP Server**

| Server Type | OpenLDAP                                                               |
|-------------|------------------------------------------------------------------------|
| Base DN     | [blank] (You need to use a specific base DN to find the user records.) |

|                                           |                                        |
|-------------------------------------------|----------------------------------------|
| Query String                              | (&(objectClass=posixAccount)(uid={u})) |
| Attribute containing the user's full name | gecos                                  |

## Group Membership Queries

AsyncOS also uses a query to determine if a user is a member of a directory group and a separate query to find all members of a group. Membership in a directory group membership determines the user's permissions within the system. When you enable external authentication on the Management Appliance > System Administration > Users page in the GUI (or `userconfig` in the CLI), you assign user roles to the groups in your LDAP directory. User roles determine the permissions that users have in the system, and for externally authenticated users, the roles are assigned to directory groups instead of individual users. For example, you can assign users in the IT directory group the Administrator role and users in the Support directory 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.

When you configure the LDAP profile to query for group membership, enter the base DN for the directory level where group records can be found, the attribute that holds the group member's username, and the attribute that contains the group name. Based on the server type that you select for your LDAP server profile, AsyncOS enters default values for the username and group name attributes, as well default query strings.



**Note**

For Active Directory servers, the default query string to determine if a user is a member of a group is `(&(objectClass=group)(member={u}))`. However, if your LDAP schema uses distinguished names in the “memberof” list instead of usernames, you can use `{dn}` instead of `{u}`.

[Table 10-7](#) shows the default query strings and attributes that AsyncOS uses when it searches for group membership information on an Active Directory server.

**Table 10-7**      **Default Query String and Attributes for Active Directory Server**

| Server Type                                                                 | Active Directory                                                                                                                                                         |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base DN                                                                     | [blank] (You need to use a specific base DN to find the group records.)                                                                                                  |
| Query string to determine if a user is a member of a group                  | (&(objectClass=group)(member={u}))<br><b>Note</b> If your LDAP schema uses distinguished names in the member of list instead of usernames, you can replace {u} with {dn} |
| Query string to determine all members of a group                            | (&(objectClass=group)(cn={g}))                                                                                                                                           |
| Attribute that holds each member's username (or a DN for the user's record) | member                                                                                                                                                                   |
| Attribute that contains the group name                                      | cn                                                                                                                                                                       |

Table 10-8 shows the default query strings and attributes that AsyncOS uses when it searches for group membership information on an OpenLDAP server.

**Table 10-8**      **Default Query String and Attributes for Open LDAP Server**

| Server Type                                                                 | OpenLDAP                                                                |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Base DN                                                                     | [blank] (You need to use a specific base DN to find the group records.) |
| Query string to determine if a user is a member of a group                  | (&(objectClass=posixGroup)(memberUid={u}))                              |
| Query string to determine all members of a group                            | (&(objectClass=posixGroup)(cn={g}))                                     |
| Attribute that holds each member's username (or a DN for the user's record) | memberUid                                                               |
| Attribute that contains the group name                                      | cn                                                                      |







# CHAPTER 11

## Configuring SMTP Routing

---

This chapter explains the features that affect routing and delivery of email traveling through the Security Management appliance.

This chapter contains the following section:

- [Routing Email for Local Domains, page 11-1](#) (SMTP Routes page and `smtproutes` command)

### Routing Email for Local Domains

The Security Management appliance routes mail to the following places:

- ISQ released messages which ignore SMTP routing
- Alerts which are be affected by SMTP routing
- Configuration files that can be mailed to the specified destination;
- Support request message that can be sent to the defined recipient as well

The last two types of messages use SMTP routes to be delivered to the destination.

The Email Security appliance routes mail to local domains to hosts specified using the **Management Appliance > Network > SMTP Routes** page (or the `smtproutes` command). This feature is similar to the sendmail **mailertable** feature. (The SMTP Routes page and `smtproutes` command are an expansion of the AsyncOS 2.0 Domain Redirect feature.)

**Note**

If you have completed the System Setup Wizard in the GUI and committed the changes, you defined the first SMTP route entries on the appliance for each RAT entry you entered at that time.

## SMTP Routes Overview

SMTP Routes allow you to redirect all email for a particular domain to a different mail exchange (MX) host. For example, you could make a mapping from `example.com` to `groupware.example.com`. This mapping causes any email with `@example.com` in the Envelope Recipient address to go instead to `groupware.example.com`. The system performs an “MX” lookup on `groupware.example.com`, and then performs an “A” lookup on the host, just like a normal email delivery. This alternate MX host does not need to be listed in DNS MX records and it does not even need to be a member of the domain whose email is being redirected. The Cisco IronPort AsyncOS operating system allows up to ten thousand (10,000) SMTP Route mappings to be configured for your Cisco IronPort appliance. (See [SMTP Routes Limits](#), page 11-4.)

This feature also allows host “globbing.” If you specify a partial domain, such as `example.com`, then any domain ending in `example.com` matches the entry. For instance, `fred@foo.example.com` and `wilma@bar.example.com` both match the mapping.

If a host is not found in the SMTP Routes table, an MX lookup is performed using DNS. The result is not re-checked against the SMTP Routes table. If the DNS MX entry for `foo.domain` is `bar.domain`, any email sent to `foo.domain` is delivered to the host `bar.domain`. If you create a mapping for `bar.domain` to some other host, email addressed to `foo.domain` is not affected.

In other words, recursive entries are not followed. If there is an entry for `a.domain` to redirect to `b.domain`, and a subsequent entry to redirect email for `b.domain` to `a.domain`, a mail loop will *not* be created. In this case, email addressed to `a.domain` will be delivered to the MX host specified by `b.domain`, and conversely email addressed to `b.domain` will be delivered to the MX host specified by `a.domain`.

The SMTP Routes table is read from the top down for every email delivery. The most specific entry that matches a mapping wins. For example, if there are mappings for both `host1.example.com` and `example.com` in the SMTP Routes

table, the entry for `host1.example.com` will be used because it is the more specific entry — even if it appears after the less specific `example.com` entry. Otherwise, the system performs a regular MX lookup on the domain of the Envelope Recipient.

## Default SMTP Route

You can also define a default SMTP route with the special keyword `ALL`. If a domain does not match a previous mapping in the SMTP Routes list, it defaults to being redirected to the MX host specified by the `ALL` entry.

When you print the SMTP Routes entries, the default SMTP route is listed as `ALL:`. You cannot delete the default SMTP route; you may only clear any values entered for it.

Configure the default SMTP route using the **Management Appliance > Network > SMTP Routes** page or the `smtproutes` command.

## Defining an SMTP Route

The Email Security appliance routes mail to local domains to hosts specified using the **Management Appliance > Network > SMTP Routes** page (or the `smtproutes` command). This feature is similar to the sendmail mailer table feature. (The SMTP Routes page and `smtproutes` command are an expansion of the AsyncOS 2.0 Domain Redirect feature.):

Use the **Management Appliance > Network > SMTP Routes** page (or the `smtproutes` command) to construct routes. When you create a new route, you first specify the domain or partial domain for which you want to create a permanent route. You then specify destination hosts. Destination hosts can be entered as fully-qualified hostnames or as IP addresses. You can also specify a special destination host of `/dev/null` to drop the messages that match the entry. (So, in effect, specifying `/dev/null` for the default route is will ensure that no mail received by the appliance is ever delivered.)

Multiple destination host entries can contain both fully-qualified hostnames and IP addresses. Separate multiple entries with commas.

If one or more of the hosts are not responding, messages will be delivered to one of the reachable hosts. If all the configured hosts are not responding, mail will be queued for that host (does not fail over to using MX records).

## SMTP Routes Limits

You can define up to 10,000 routes. The final default route of `ALL` is counted as a route against this limit. Therefore, you can define up to 9,999 custom routes and one route that uses the special keyword `ALL`.

## SMTP Routes and DNS

Use the special keyword `USEDNS` to tell the appliance to do MX lookups to determine next hops for specific domains. This is useful when you need to route mail for subdomains to a specific host. For example, if mail to `example.com` is to be sent to the company's Exchange server, you might have something similar to the following SMTP route:

```
example.com exchange.example.com
```

However, for mail to various subdomains (`foo.example.com`), add an SMTP route that looks like this:

```
.example.com USEDNS
```

## SMTP Routes and Alerts

Alerts sent from the appliance to addresses specified on the Security Management appliance from **Management Appliance > System Administration > Alerts** page (or the `alertconfig` command) follow SMTP Routes defined for those destinations.

## SMTP Routes, Mail Delivery, and Message Splintering

Incoming: if one message has 10 recipients and they are all on the same Exchange server, AsyncOS will open one TCP connection and present exactly one message to the mail store, not 10 separate messages.

Outgoing: works similarly, but if one message is going to 10 recipients in 10 different domains, AsyncOS will open 10 connections to 10 MTAs and deliver them one email each.

Splintering: if one incoming message has 10 recipients and they are each in separate Incoming Policy groups (10 groups), the message will splinter even if all 10 recipients are on the same Exchange server. Thus, 10 separate emails will be delivered over a single TCP connection.

## SMTP Routes and Outbound SMTP Authentication

If an Outbound SMTP Authentication profile has been created, you can apply it to an SMTP Route. This allows authentication for outgoing mail in cases where the Cisco IronPort appliance sits behind a mail relay server that is at the edge of the network.

## Managing SMTP Routes on the Security Management Appliance

To manage SMTP routes on the Security Management appliance, perform the following:

- Step 1** On the Security Management appliance, choose **Management Appliance > Network > SMTP Routes**.

The SMTP Routes page appears.

**Figure 11-1** *SMTP Routes Page*

### SMTP Routes

| SMTP Routes List                 |                       |                                                                   |
|----------------------------------|-----------------------|-------------------------------------------------------------------|
| <a href="#">Add Route...</a>     |                       | <a href="#">Clear All Routes</a> <a href="#">Import Routes...</a> |
| Receiving Domain                 | Destination Hosts     | All <input type="checkbox"/> Delete                               |
| .example.com                     | exchange4.example.com | <input type="checkbox"/>                                          |
| All Other Domains                |                       |                                                                   |
| <a href="#">Export Routes...</a> |                       | <a href="#">Delete</a>                                            |

Use this page to manage SMTP Routes on your Cisco IronPort appliance. From this page you can add, modify, and delete mappings in the table. You can export or import the SMTP Routes entries.

## Adding SMTP Routes

To add an SMTP Route, perform the following:

**Step 1** On the Security Management appliance, choose **Management Appliance > Network > SMTP Routes**.

**Step 2** Click **Add Route**.

The Add SMTP Route page is displayed:

**Figure 11-2 Add SMTP Route Page**

### Add SMTP Route

| SMTP Route Settings                                                         |                                                                                                                                                                                                                                               |                  |  |                      |                                                                              |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--|----------------------|------------------------------------------------------------------------------|
| Receiving Domain: ?                                                         | <input type="text"/>                                                                                                                                                                                                                          |                  |  |                      |                                                                              |
| Destination Hosts: ?                                                        | <table border="1"> <thead> <tr> <th>Destination Host</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td> <input type="button" value="Add Row"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table> | Destination Host |  | <input type="text"/> | <input type="button" value="Add Row"/> <input type="button" value="Delete"/> |
|                                                                             | Destination Host                                                                                                                                                                                                                              |                  |  |                      |                                                                              |
| <input type="text"/>                                                        | <input type="button" value="Add Row"/> <input type="button" value="Delete"/>                                                                                                                                                                  |                  |  |                      |                                                                              |
| Outgoing SMTP Authentication: ?                                             | <input type="text"/>                                                                                                                                                                                                                          |                  |  |                      |                                                                              |
| No Outgoing SMTP Authentication Profiles Configured                         |                                                                                                                                                                                                                                               |                  |  |                      |                                                                              |
| <input type="button" value="Cancel"/> <input type="button" value="Submit"/> |                                                                                                                                                                                                                                               |                  |  |                      |                                                                              |

**Step 3** Enter a receiving domain and destination host. You can add multiple destination hosts by clicking **Add Row** and entering the next destination host in the new row.

**Step 4** You can specify a port number by adding “:<port number>” to the destination host: `example.com:25`

**Step 5** Click **Submit**.

**Step 6** The SMTP Routes page is displayed, reflecting your changes.

**Step 7** Click **Commit Changes**, add an optional comment if necessary, and then click **Commit Changes**.

## Editing SMTP Routes

To edit an SMTP Route, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Network > SMTP Routes**.
- Step 2** Click the name of an existing SMTP Route in the SMTP Route listing.  
The Edit SMTP Route page is displayed.
- Step 3** Edit the route.
- Step 4** Click **Submit**.
- Step 5** The SMTP Routes page is displayed, reflecting your changes.
- Step 6** Click **Commit Changes**, add an optional comment if necessary, then click **Commit Changes**.
- 

## Deleting SMTP Routes

To delete SMTP Routes, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > Network > SMTP Routes**.
- Step 2** Select the check boxes to the right of the SMTP Routes to delete.
- Step 3** Click **Delete**.  
To delete all of the SMTP Routes, select the check box labeled “All” and click **Delete**.
- 

## Exporting SMTP Routes

Similar to the Host Access Table (HAT) and the Recipient Access Table (RAT), you can also modify SMTP routes mappings by exporting and importing a file. To export the SMTP Routes:

- 
- Step 1** Click **Export SMTP Routes** on the SMTP Routes page. The Export SMTP Routes page is displayed.

- Step 2** Enter a name for the file and click **Submit**.
- 

## Importing SMTP Routes

Similar to the Host Access Table (HAT) and the Recipient Access Table (RAT), you can also modify SMTP routes mappings by exporting and importing a file. To import SMTP Routes:

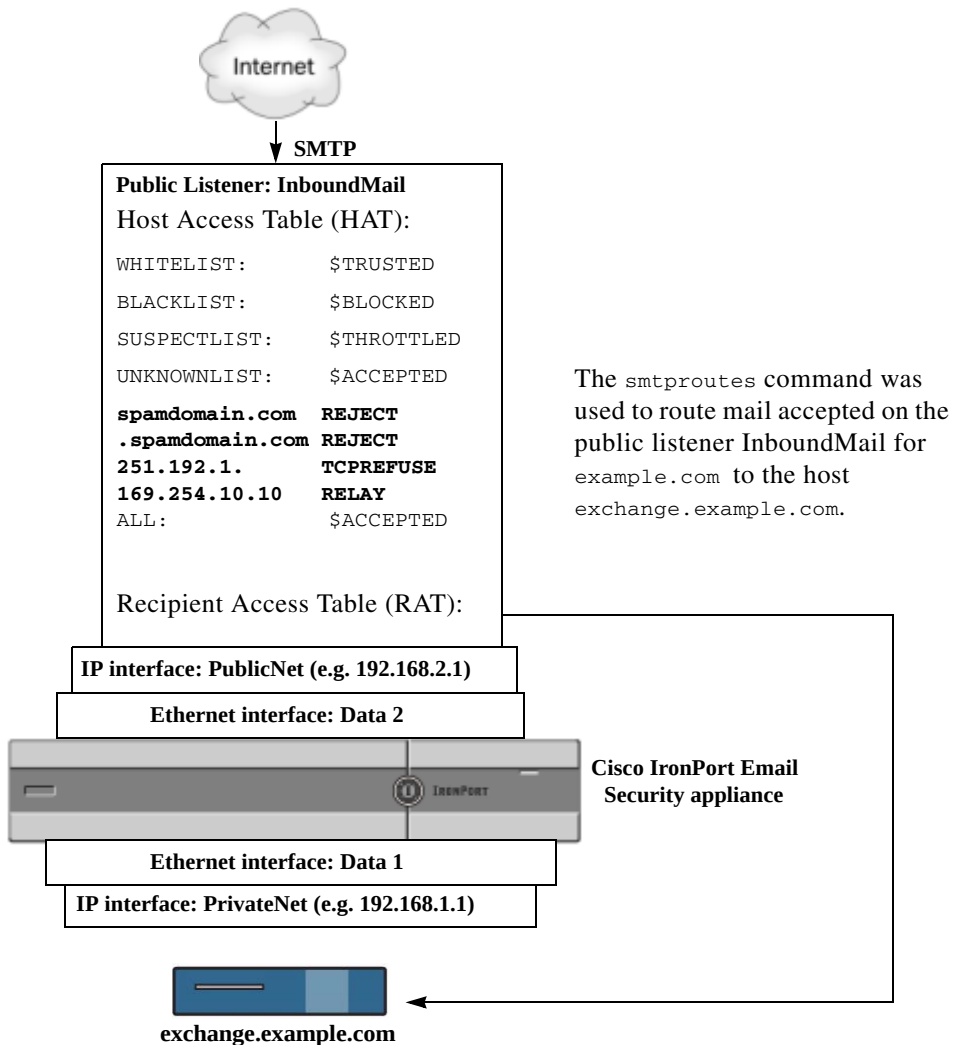
- 
- Step 1** Click **Import SMTP Routes** on the SMTP Routes page. The Import SMTP Routes page is displayed.
- Step 2** Select the file that contains the exported SMTP Routes.
- Step 3** Click **Submit**. You are warned that importing will replace all existing SMTP Routes. All of the SMTP Routes in the text file are imported.
- Step 4** Click **Import**.

You can place “comments” in the file. Lines that begin with a ‘#’ character are considered comments and are ignored by AsyncOS. For example:

```
# this is a comment, but the next line is not  
ALL:
```

At this point, our Email Gateway configuration looks like this:



**Figure 11-3 SMTP Routes Defined for a Public Listener**





# CHAPTER 12

## Common Administrative Tasks

---

You can perform most system administration tasks by using the System Administration menu in the graphical user interface (GUI). Some system administration features, however, are available only in the command line interface (CLI).

In addition, you access the status-monitoring features of the appliance on the Monitor menu, which is described in [Chapter 9, “Monitoring System Status.”](#)



### Note

---

Several of the features or commands described in this chapter can affect routing precedence. For more information, see [IP Addresses, Interfaces, and Routing, page B-3](#).

---

This chapter contains the following sections:

- [Performing Maintenance Tasks Using CLI Commands, page 12-2](#)
- [Backing Up Your Security Management Appliance, page 12-8](#)
- [Upgrading to New Security Management Appliance Hardware, page 12-15](#)
- [Upgrading AsyncOS, page 12-17](#)
- [Configuring Upgrade and Service Update Settings, page 12-32](#)
- [Disaster Recovery on the Security Management Appliance, page 12-36](#)
- [About Distributing Administrative Tasks, page 12-40](#)
- [Configuring Access to the Security Management Appliance, page 12-70](#)
- [Viewing Active Sessions, page 12-75](#)
- [Configuring the Return Address for Generated Messages, page 12-76](#)

- [Managing Alerts, page 12-76](#)
- [Changing Network Settings, page 12-89](#)
- [Configuring the System Time, page 12-98](#)
- [Managing the Configuration File, page 12-103](#)
- [Managing Disk Usage, page 12-115](#)

## Performing Maintenance Tasks Using CLI Commands

The operations and commands described in this section enable you to perform maintenance-related tasks on the Security Management appliance. This section describes the following operations and commands:

- **shutdown**
- **reboot**
- **suspend**
- **offline**
- **resume**
- **resetconfig**
- **version**

## Shutting Down the Security Management Appliance

To shut down your Security Management appliance, use the **Management Appliance > System Administration > Shutdown/Reboot** page, or use the **shutdown** command at the command line prompt.

Shutting down an appliance exits 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 shut down. The default delay is 30 seconds. AsyncOS allows open connections to complete during the delay, after which it forcefully closes open connections.

## Rebooting the Security Management Appliance

To reboot your Security Management appliance, use the Shutdown/Reboot page available on the System Administration menu in the GUI, or use the `reboot` command in the CLI.

Rebooting your appliance restarts AsyncOS, which allows you to safely power down and reboot the appliance. You must enter a delay for the appliance to shut down. The default delay is 30 seconds. 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.

## Placing the Security Management Appliance into a Maintenance State

If you want to perform system maintenance, place the Security Management appliance into the offline state. The `suspend` and `offline` commands put AsyncOS 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 30 seconds. 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.

See also:

- “Suspending Email Delivery,” “Resuming Email Delivery,” “Suspending Receiving,” and “Resuming Receiving” in the *Cisco IronPort AsyncOS for Email Advanced User Guide*

## 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 returns AsyncOS to normal operating state after using the `suspenddel` or `suspend` command.

## 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 **Management Appliance > System Administration > Configuration File** page, or the `resetconfig` command, resets *all* 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 that you run the System Setup Wizard after resetting the configuration.



### Note

The `resetconfig` command works only when the appliance is in the offline state. When the `resetconfig` command completes, the appliance is automatically returned to the online state. 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, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Management Appliances > Centralized Services > System Status**.
- Step 2** Scroll to the bottom of the page and look under Version Information to see the version of AsyncOS that is currently installed.
- Additionally, you can use the **version** command at the command line prompt.
- 

## Backing Up Your Security Management Appliance

- [About Backing Up Your Data, page 12-8](#)
- [Restrictions for Backups, page 12-9](#)
- [Backup Duration, page 12-10](#)
- [Availability of Services During Backups, page 12-10](#)
- [Interruption of a Backup Process, page 12-11](#)
- [Scheduling a Backup, page 12-11](#)
- [Other Important Backup Tasks, page 12-15](#)

## About Backing Up Your Data

The Security Management appliance allows you to copy its active data set from the ‘source’ appliance to a ‘target’ Security Management appliance with minimum disruption on the originating ‘source’ Security Management appliance. The Security Management appliance does not consider one machine to be a ‘primary’ or ‘backup’ appliance, but rather ‘source’ and ‘target’ appliances. That

is, the machine that is sending data is the ‘source’, and the appliance that has received the data from another Security Management appliance as part of a scheduled backup is the ‘target’.

Once the data transfer is finished the data on the two boxes will be identical. Backed-up data includes web tracking and trend reporting, email reporting, Message Tracking, Cisco IronPort Spam Quarantine, and Safelist/Blocklist data. Configurations and logs are not backed up using this process.

The backup feature provides you with the **backupconfig** command that allows you to back up your data files without using the Security Management appliance GUI. Additionally, you can view or cancel scheduled and ongoing backups, check the status of a backup, or verify if a backup can be scheduled onto a remote machine.

## Restrictions for Backups

Be sure to address the following restrictions before you schedule a backup:

| Restriction                               | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance capacity                        | The capacity of the target appliance must be the same as or greater than the capacity of the source appliance.                                                                                                                                                                                                                                                                                                                                                        |
| Appliance version                         | AsyncOS 7.7 for Security Management data can be backed up only to another appliance running AsyncOS 7.7 for Security Management. If there is a version incompatibility, upgrade the target Security Management appliance before scheduling a backup.                                                                                                                                                                                                                  |
| Multiple, concurrent, and chained backups | <p>Data from a Security Management appliance can be backed up to exactly one Security Management appliance.</p> <p>Chained backup (a backup to a backup) is not supported.</p> <p>If a backup is scheduled to or from a Security Management appliance, you cannot schedule another backup to or from that Security Management appliance. To schedule backups to another Security Management appliance, first cancel any current ongoing backup or future backups.</p> |

## Backup Duration

During a full initial backup, a backup of 800GB may take up to 10 hours. Daily backups, may take up to 3 hours each. Weekly and monthly backups may take longer. These numbers may vary.

After the initial backup, the backup process transfers only files that have changed since the last backup. Thus, subsequent backups should take less time than the initial backup. The time required for subsequent backups depends on the amount of data accumulated, how many files have changed, and to what extent the files have changed since the last backup.

## Availability of Services During Backups

The phases of the backup process and their effect on the availability of services are as follows:

- Phase 1—Phase 1 of the backup process starts with the data transfer between the source and target appliances. During data transfer, services on the source appliance remain running, therefore data collection can still continue. However, services are shut down on the target appliance. Once the data transfer is complete from the source to target appliance, Phase 2 begins.
- Phase 2—When Phase 2 begins, services on the source appliance are shut down. Any differences that have collected during the data transfer between the source and target appliance since the initial shutdown are copied to the target appliance and the service is brought back up for both the source and the target. This allows maintain maximum uptime on the source appliance and no data loss for either appliance.

During the backup, data availability reports may not work, and when viewing the message tracking results, the hostname for each message may be labeled as ‘unresolved’.

If you try to schedule a report and forget that a backup is in progress, you can check the system status by choosing **Management Appliance > Centralized Services**. From this window you can see the warning that a system backup is in progress:

The screenshot shows the 'Management Appliance' configuration page. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below these are sub-tabs for 'Centralized Services', 'Network', and 'System Administration'. A warning message states: 'System backup in progress. Some services may be temporarily unavailable. [More Information](#)'. A 'Commit Changes >' button is in the top right. The main section is titled 'Security Appliances'. Under 'Centralized Service Status', there is a table:

| Centralized Service Status   |                           |
|------------------------------|---------------------------|
| Configuration Manager (Web): | Enabled, using 0 licenses |
| Spam Quarantine:             | Enabled, using 0 licenses |
| Reporting:                   | Service disabled          |
| Tracking:                    | Enabled, using 0 licenses |

Below this is the 'Security Appliances' section with an 'Email' sub-tab. It contains an 'Add Email Appliance...' button and the text 'No appliances have been added.' At the bottom, there is a 'Web' sub-tab and a 'Done' button.

## Interruption of a Backup Process



### Note

If there is an unexpected reboot of the source appliance while a backup is being performed, the target appliance is unaware of this stoppage. You must cancel the backup on the target appliance.

If there is an interruption of the backup process and the backup process is not completed, the next time a backup is attempted, the Security Management appliance can start the backup process up from where it was stopped. When a backup is cancelled, the backup process does not erase the data it has already backed up onto the target machine.

## Scheduling a Backup



### Note

A backup process will not start if there are any ongoing backups on the remote machine.

There are two type of scheduled backups that you can perform on the Security Management appliance:

- **Periodic Backups**—Periodic backups consist of continual backups that can be scheduled for a predetermined time, or for a single backup that occurs at a predetermined time.
- **Immediate Backups**—Instant backups occur immediately when you initiate the **backupconfig** command on the CLI.

## Periodic Backups



### Note

Log files can also be saved on a periodic basis. For more information on this process, see [Log Subscriptions, page 13-36](#).

To schedule periodic backups, perform the following steps.

---

**Step 1** Login, as administrator, to any SSH session.

**Step 2** At the command prompt, type **backupconfig** and press **Enter**.

Choose the operation you want to perform:

- View—Allows you to view the scheduled backups
- Verify—Verifies whether the backup can be scheduled to a remote machine.
- Schedule—Allows you to schedule a backup to an appliance.
- Cancel—Cancels a scheduled backup.
- Status—Allows you to view the status of the ongoing back up in progress.

**Step 3** At the command prompt, type **Schedule** and press **Enter**.

**Step 4** Type the IP address and name of the target Security Management appliance.

The Security Management appliance now verifies the existence of the target machine, and determines whether the target machine has enough space to accept the data.

If the space on the target machine is not sufficient, the following error message is generated "Backup cannot be scheduled. Reason: There is not enough space for isq, tracking, reporting, slbl. Please increase disk allocation for these services on the target machine" and data is not transferred.

Once the target machine is verified, the following choices appear:

1. Setup Repeating Backup Schedule—allows you schedule a periodic backup.
2. Schedule a single backup—allows you to schedule a single backup.
3. Start a Single Backup—allows you to initiate an immediate backup.

**Step 5** Type **1** and press **Enter**.

The following choices appear: 1. Daily, 2. Weekly, 3. Monthly.

**Step 6** Choose the time frame for your periodic backup and press **Enter**.

**Step 7** Type the specific time and/or date that you want the backup to start and press **Enter**.

**Step 8** Type the name of the backup process.

This can be any name that is meaningful to you so that later on you can verify this backup process.

This is Phase 1 of the backup.

Type **Status** at the command line prompt, and you will see the following:

```
Phase: One
Centralized Email Tracking: Completed
Centralized Spam Quarantine: Completed
Centralized Email Reporting: Completed
Centralized Web Reporting: In Progress
```

This output indicates that data is being transferred to the new target machine.

At the end of Phase 2, the data transfer is complete. Type **Status** at the command line prompt, and you will see the following:

```
Phase: Two
Centralized Email Tracking: Completed
Centralized Spam Quarantine: Completed
Centralized Email Reporting: Completed
Centralized Web Reporting: Completed
```

**Step 9** When data transfer is complete, verify that the backup was successfully scheduled: Type **View** and press **Enter** at the command prompt.

**Step 10** For a complete backup, see [Other Important Backup Tasks, page 12-15](#).

## Immediate Backups

Perform the following steps to start an instant backup.



### Note

All directions listed below are to be typed at the command prompt.

**Step 1** Login, as administrator, to any SSH session.

**Step 2** At the command prompt, type **backupconfig** and press **Enter**.

Choose the operation you want to perform:

- View—Allows you to view the scheduled backups.
- Verify—Verifies if the backup can be scheduled to a remote machine.
- Schedule—Allows you to schedule a backup to an appliance.
- Cancel—Cancels a scheduled backup.
- Status—Allows you to view the status of the ongoing back up in progress.

**Step 3** Type **Schedule** and press **Enter**.

**Step 4** Type the IP address and name of the target Security Management appliance.

The Security Management appliance now verifies the existence of the target machine, and determines whether the target machine has enough space to accept the data.

If the space on the target machine is not sufficient, the following error message is generated "Backup cannot be scheduled. Reason: There is not enough space for isq, tracking, reporting, slbl. Please increase disk allocation for these services on the target machine" and data is not transferred.

Once the target machine is verified, the following choices appear on the console:

1. Setup Reoccurring Backup—allows you schedule a periodic backup.
2. Schedule a Single backup—allows you to schedule a single backups.
3. Start a Single Backup Now—allows you to initiate an immediate backup.



**Step 5** Type **3** and press **Enter**.

The backup process begins, and data instantly starts transferring from the source machine to the target machine. After an immediate backup has started, the following message can be seen: "Backup has been initiated and will begin in a few seconds."

**Step 6** To verify that the backup was successfully scheduled, type **View** or **Status** and press **Enter** at the command prompt.

**Step 7** For a complete backup, see [Other Important Backup Tasks, page 12-15](#).

---

## Other Important Backup Tasks

Consider doing the following in order to prevent loss of items that are not backed up by the backup processes described in this section:

- To save your configuration settings, see [Managing the Configuration File, page 12-103](#).
- To save log files from your Security Management appliance to an alternate location, see [Chapter 13, "Logging."](#)

## Upgrading to New Security Management Appliance Hardware

If you are upgrading from an older Security Management appliance to a newer model, for example, upgrading from an M160 to an M650, perform the following steps to transfer the data from the older appliance to the new appliance successfully.

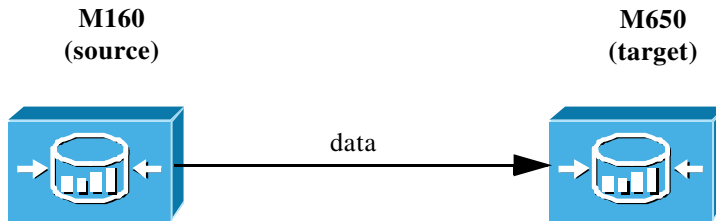


### Note

It is important to remember that while it is possible to transfer data between Security Management appliances that are different sizes, the new appliance must have the same size allocations or greater.

---

**Figure 12-1**      **Upgrading to a New Security Management Appliance Hardware**



**Note**

All directions listed below are to be typed at the command prompt.

**Step 1**      Login, as administrator, to any SSH session.

**Step 2**      At the command prompt, type **backupconfig** and press **Enter**.

Choose the operation you want to perform:

- View—Allows you to view the scheduled backups
- Verify—Verifies whether the backup can be scheduled to a remote machine.
- Schedule—Allows you to schedule a backup to an appliance.
- Cancel—Cancels a scheduled backup.
- Status—Allows you to view the status of the ongoing back up in progress.

**Step 3**      Type **Schedule** and press **Enter**.

**Step 4**      Type the IP address and name of the target Security Management appliance.

The Security Management appliance now verifies the existence of the target machine, and if the target machine has enough space to accept the data.

It is possible to transfer data between Security Management appliances that are different sizes, but, the new appliance must have the same size allocations or greater. If the space on the target machine is not sufficient, the following error message is generated **“Backup cannot be scheduled. Reason: There is not enough space for isq, tracking, reporting, sbl. Please increase disk allocation for these services on the target machine”** and data is not transferred.

Once the target machine is verified, the following choices appear on the console:

- 1. Setup Reoccurring Backup—allows you schedule a periodic backup.

- 2. Schedule a Single backup—allows you to schedule a single backups.
- 3. Start a Single Backup Now—allows you to initiate an immediate backup.

**Step 5** Type **3** and press **Enter**.

The backup process begins, and data instantly starts transferring from the source machine to the target machine. After an immediate backup has started, the following message can be seen: "Backup has been initiated and will begin in a few seconds."

**Step 6** Suspend all data transfer between the source appliance and the new target appliance by typing the **suspendtransfers** command at the command line prompt.

The **suspendtransfers** command stops the older source Security Management appliance from receiving any data.

**Step 7** Run a new instant backup on the source machine by repeating steps 2 through 5 above.

## Upgrading AsyncOS

This section discusses the following topics related to software upgrades on the Security Management appliance:

- [Before You Upgrade: Important Steps, page 12-17](#)
- [Upgrading AsyncOS from the GUI, page 12-23](#)
- [Reverting to an Earlier Version of AsyncOS, page 12-25](#)
- [Obtaining Upgrades Using the CLI, page 12-29](#)

## Before You Upgrade: Important Steps

Prepare for an upgrade by taking the following steps:

---

**Step 1** Take steps to prevent data loss:

- Make sure the new appliance has sufficient disk capacity and the same or greater size allocations for each data type that will be transferred. See [Maximum Disk Space Available, page 12-116](#).

- If you have received any disk space warnings, resolve any disk space issues before upgrading.

**Step 2** Save the XML configuration file off the appliance.

**Step 3** If you are using the Safelist/Blocklist feature, export the list off the appliance.

**Step 4** Suspend the listeners using the **suspendlistener** command when running the upgrade from the CLI. If you perform the upgrade from the GUI, listener suspension occurs automatically.

**Step 5** Drain the mail queue and the delivery queue.




---

**Note** Re-enable the listeners after the upgrade.

---

Before upgrading AsyncOS, verify the upgrade and update settings are configured correctly. For more information, see [Configuring Upgrade and Service Update Settings, page 12-32](#).

## Remote vs. Streaming Upgrades

Cisco IronPort provides two methods (or ‘sources’) for upgrading AsyncOS on your Cisco IronPort appliances: Remote upgrades and Streaming upgrades.

In Remote upgrades, your Cisco IronPort appliances download the AsyncOS upgrades from a server within your network. You only download the upgrade image from Cisco IronPort one time, and then serve it to your Cisco IronPort appliances.

With Streaming upgrades, your Cisco IronPort appliances download the AsyncOS upgrades via HTTP directly from the Cisco IronPort update servers. Each Cisco IronPort appliance downloads the upgrade separately.

Cisco IronPort Systems uses a distributed upgrade server architecture to make sure customers can quickly download AsyncOS upgrades wherever in the world they are located. Because of this distributed server architecture, the Cisco IronPort update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for AsyncOS upgrades. If you determine that your firewall settings require a static IP for upgrades, contact Cisco IronPort Customer support to obtain the required URL addresses.

**Note**

If you have any existing firewall rules allowing download of legacy upgrades from `upgrades.cisco.com` ports such as 22, 25, 80, 4766, they will need to be removed and/or replaced with revised firewall rules.

Use the **Management Appliance > System Administration > Update Settings** page to switch between the two upgrading methods (Streaming is the default). Optionally, use the **updateconfig** command in the CLI.

When upgrading, do not pause for long amounts of time at the various prompts. If the TCP session should happen to time out during the download, your upgrade may fail.

**Note**

Regardless of which upgrade method you use, you should also consider saving your configuration using the **saveconfig** command after your upgrade is complete. For more information, see [Managing the Configuration File, page 12-103](#).

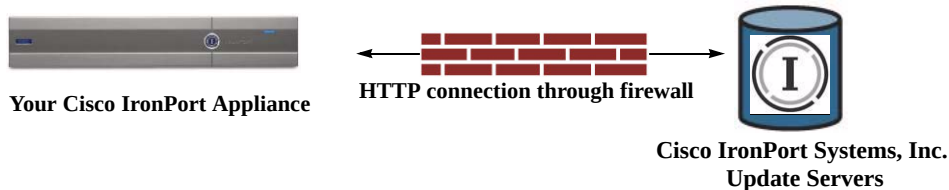
## Upgrading Clustered Systems

If you are upgrading clustered machines, see “Upgrading Machines in a Cluster” in the Centralized Management chapter in the *Cisco IronPort AsyncOS for Email Advanced User Guide*.

## Streaming Upgrade Overview

In Streaming upgrades, your Cisco IronPort appliance connects directly to the Cisco IronPort update servers to find and download upgrades:

**Figure 12-2 Streaming Update Method**

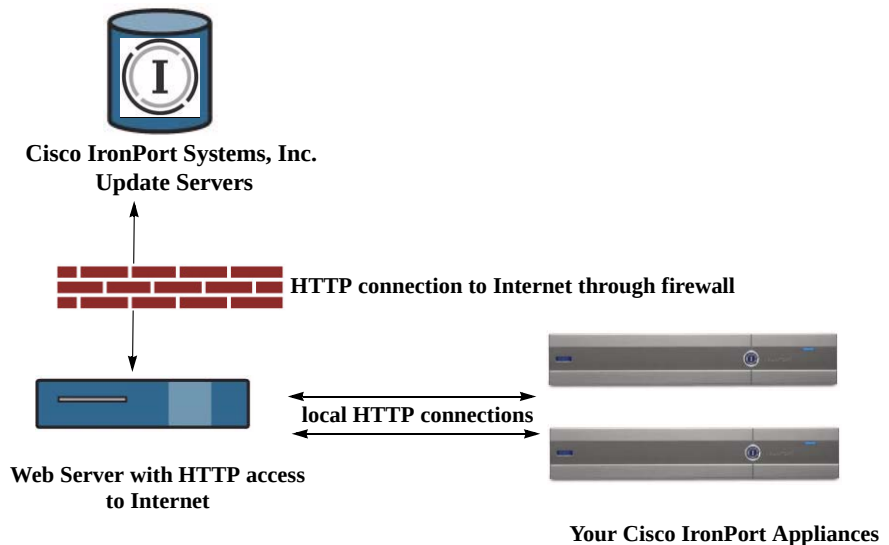


This method requires that your Cisco IronPort appliance contacts the Cisco IronPort Systems update servers directly from the network.

## Remote Upgrade Overview

You can also download and host updates to AsyncOS locally from within your own network (Remote Upgrade) rather than obtaining updates directly from Cisco IronPort's update servers (Streaming Upgrades). Using this feature, an encrypted update image downloaded via HTTP to any server in your network that has access to the Internet. If you choose to download the update image, you can then configure an internal HTTP server (an "update manager") to host the AsyncOS images to your Cisco IronPort appliances.

**Figure 12-3 Remote Update Method**



The basic process is as follows:

- 
- Step 1** Configure a local server to retrieve and serve the upgrade files.
  - Step 2** Download the upgrade files.
  - Step 3** Choose **Management Appliance > System Administration > Update Settings**

From this page, choose to configure the appliance to use the local server.

**Step 4** Choose **Management Appliance > System Administration > System Upgrade**

**Step 5** Click **Available Upgrades**.



**Note**

From the command line prompt you can also do the following:  
Run the **updateconfig** command then run the **upgrade** command.

## Hardware and Software Requirements for Remote Upgrades

For *downloading* AsyncOS upgrade files, you must have a system in your internal network that has:

- Internet access to the Cisco IronPort Systems update servers.
- A web browser.



**Note**

For this release, if you need to configure a firewall setting to allow HTTP access to this address, you must configure it using the DNS name and not a specific IP address.

For *hosting* AsyncOS update files, you must have a server in your internal network that has:

- A web server — for example, Microsoft IIS (Internet Information Services) or the Apache open source server — that:
  - supports the display of directory or filenames in excess of 24 characters
  - has directory browsing enabled
  - is configured for anonymous (no authentication) or basic (“simple”) authentication
  - contains at least 350MB of free disk space for each AsyncOS update image

## Hosting a Remote Upgrade Image

After setting up a local server, go to

**[http://updates.ironport.com/fetch\\_manifest.html](http://updates.ironport.com/fetch_manifest.html)** to download a zip file of an upgrade image. To download the image, enter your serial number and the version number of the Cisco IronPort appliance. You will then be presented with a list of available upgrades. Click the upgrade version that you want to download a zip file of the upgrade image. To use the upgrade image for AsyncOS upgrades, enter the base URL for your local server on the Edit Update Settings page (or use `updateconfig` in the CLI).

You can also host an XML file on a local server that limits the available upgrades for the Cisco IronPort appliances on your network to the version selected at [http://updates.ironport.com/fetch\\_manifest.html](http://updates.ironport.com/fetch_manifest.html). Your Cisco IronPort appliances still download the upgrade from the Cisco IronPort Systems update servers. If you want to host the upgrade list on a local server, download the zip file and extract the `asyncos/phoebe-my-upgrade.xml` file to the root directory of the local server. To use the upgrade list for AsyncOS upgrades, enter the full URL for the XML file on the Edit Update Settings page (or use `updateconfig` in the CLI).

For more information about remote upgrades, see the Cisco IronPort Knowledge Base or contact your Cisco IronPort Support provider.

## Obtaining Upgrades Using the GUI

To specify where to retrieve upgrades (either streaming or local sources), choose **Management Appliance > System Administration > Update Settings** on the Security Management appliance.



**Figure 12-4 The Update Settings Page****Update Settings**

| Update Settings for Security Services   |                           |                                      |
|-----------------------------------------|---------------------------|--------------------------------------|
| Update Server (images):                 | IronPort Update Server    |                                      |
| Update URLs:                            | Service                   | Update URL                           |
|                                         | Feature Key updates       | http://downloads.ironport.com/asynco |
|                                         | IronPort AsyncOS upgrades | IronPort Servers                     |
| Update Server (list):                   | IronPort Update Server    |                                      |
| Update URLs:                            | Service                   | Update URL                           |
|                                         | IronPort AsyncOS upgrades | Dynamic                              |
| Interface:                              | Auto Select               |                                      |
| HTTP Proxy Server:                      | Not Enabled               |                                      |
| HTTPS Proxy Server:                     | Not Enabled               |                                      |
| <a href="#">Edit Update Settings...</a> |                           |                                      |

## Upgrading AsyncOS from the GUI

To upgrade AsyncOS after you have configured your update settings, perform the following:

- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > System Upgrade > Available Upgrades**.

The Available Upgrades page appears.

**Figure 12-5 Available Upgrades Page****Available Upgrades**

| Upgrades                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Select an upgrade from the list below. Most system upgrades require a reboot of the system after the upgrade is applied. Changes made to your system's configuration between the time the upgrade download is completed and the system is rebooted will not be saved.</p>                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>Available Upgrades:</p> <ul style="list-style-type: none"> <li>Turn AsyncOS appliance into LDAP-MySQL proxy (build 007)</li> <li>Remove seed keys from Hosted appliance</li> <li>GrowFS utility to increase available RAID size (build 002)</li> <li>AsyncOS 7.2.0 build 151 upgrade For Email, 2010-03-17</li> <li>AsyncOS 7.2.0 build 150 upgrade For Email, 2010-03-16</li> <li>AsyncOS 7.2.0 build 149 upgrade For Email, 2010-03-15</li> </ul> | <p>Upgrade Preparation:</p> <p><input checked="" type="checkbox"/> Save the current configuration to the <i>configuration</i> directory before upgrading.</p> <p><input checked="" type="checkbox"/> Mask passwords in the configuration file.<br/> <small>Note: Files with masked passwords cannot be loaded using Load Configuration.</small></p> <p>Email file to: <input type="text"/></p> <p><small>Separate multiple addresses with commas.</small></p> |
| <p style="text-align: left;"><a href="#">Cancel</a></p> <p style="text-align: right;"><a href="#">Begin Upgrade &gt;</a></p>                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

- Step 2** Select an upgrade from the list of available upgrades.

**Step 3** In the Upgrade Preparation section, check the checkbox if you want to save the current configuration to the configuration directory before upgrading. This is recommended.

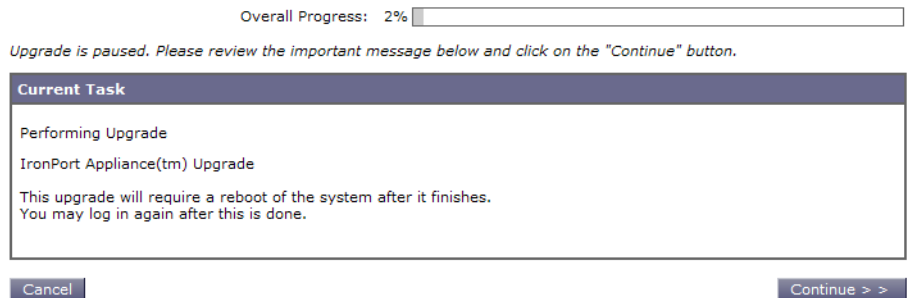
In this section you can also hide the passwords in the configuration file by checking Mask Passwords in the Configuration File checkbox. Additionally, you can email this password file to an email of your choice by entering the email address in the text field.

**Step 4** Click **Begin Upgrade**. A progress bar appears near the top of the page.

**Step 5** If prompted, confirm changes or read and agree to new license agreements.

**Figure 12-6 Upgrade Progress**

### System Upgrade

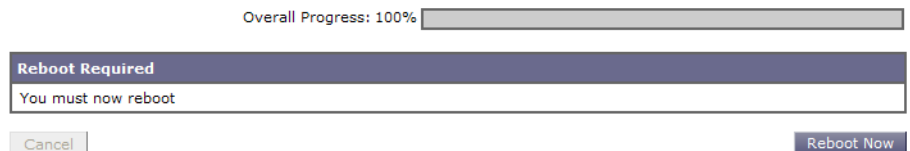


**Step 6** Click **Continue** to complete the upgrade.

**Step 7** After the upgrade is finished, you are prompted to reboot the appliance.

**Figure 12-7 Upgrade Complete**

### System Upgrade



**Step 8** Click **Reboot Now**.

**Step 9** When the appliance comes up again, sign in.

- Step 10** If you are upgrading from a release earlier than AsyncOS 7.2: The first time you click the Web tab, you will be prompted to initialize the latest Configuration Master. For information, see [Initializing Configuration Masters, page 8-7](#).
- 

## Reverting to an Earlier Version of AsyncOS

You can revert to an to a previous qualified version of AsyncOS for emergency uses.

Because upgrades cause one-way transformation of key subsystems, the reversion process is complex and requires qualification by Cisco IronPort Quality Assurance teams. You can revert to one of the previous two versions only. The earliest AsyncOS version supported for this functionality is AsyncOS 6.5; prior versions of AsyncOS are not supported.

### Important Note About Reversion Impact

Using the `revert` command on a Cisco IronPort appliance is a very destructive action. This command destroys all configuration logs and databases. In addition, it disrupts mail handling until the appliance is reconfigured. Because this command destroys all configuration, it is highly recommended that you have physical local access to the Cisco IronPort appliance when you want to issue the `revert` command.



#### Warning

---

**You must have a configuration file for the version you want to revert to. Configuration files are *not* backwards-compatible.**

---

## Performing the AsyncOS Reversion

To revert to a previous qualified version of AsyncOS:

- 
- Step 1** Ensure that you have the configuration file for the version you want to revert to. Configuration files are not backwards-compatible.

- Step 2** Save a backup copy of the current configuration of your appliance (with passwords unmasked) on another machine. To do this, you can email the file to yourself or FTP the file. A simple way to do this is to run the `mailconfig` CLI command, which emails the current configuration file on your appliance to the specified email address.




---

**Note** This is not the configuration file you will load after reverting.

---

- Step 3** If you use the Safelist/Blocklist feature, export the Safelist/Blocklist database to another machine.
- Step 4** Suspend any listeners on your Email Security appliances.
- Step 5** Wait for the mail queue to empty.
- Step 6** Log in to the CLI of the appliance you want to revert.
- When you run the `revert` command, several warning prompts are issued. Once these warning prompts are accepted, the revert action takes place immediately. Therefore, do not begin the reversion process until after you have completed the prereversion steps.
- Step 7** From the command line prompt, type the **revert** command and respond to the prompts.

The following example shows the **revert** command:

```
m650p03.prep> revert
```

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.

The following data will be destroyed in the process:

- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy

quarantines)

- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco IronPort Spam Quarantine message and end-user safelist/blocklist data

Only the network settings will be preseved.

Before running this command, be sure you have:

- saved the configuration file of this appliance (with passwords unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.

After rebooting, the appliance reinitializes itself and reboots again to the desired version.

Do you want to continue? **yes**

Are you sure you want to continue? **yes**

```
Available versions
```

```
=====
```

1. 7.2.0-390
2. 6.7.6-020

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

```
You have selected "7.2.0-390".
```

```
Reverting to "testing" preconfigure install mode.
```

```
The system will now reboot to perform the revert operation.
```

- Step 8** Wait for the appliance to reboot twice.
  - Step 9** Log in to the appliance using the CLI.
  - Step 10** Load the XML configuration file of the version you are reverting to.
  - Step 11** If you use the Safelist/Blocklist feature, import and restore the Safelist/Blocklist database.
  - Step 12** Reenable any listeners on your Email Security appliances.
  - Step 13** Commit your changes.
- The reverted Cisco IronPort appliance should now run using the selected AsyncOS version.

**Note**

It may take 15 to 20 minutes before reversion is complete and console access to the Cisco IronPort appliance is available again.

## Obtaining Upgrades Using the CLI

To specify where to retrieve the AsyncOS upgrade (locally or from the Cisco IronPort servers), run the `updateconfig` command. To install an upgrade, run the `upgrade` command.



### Note

In previous versions of AsyncOS, the `upgradeconfig` command was used to retrieve upgrades to AsyncOS. This command is no longer used.

## The updateconfig Command

The `updateconfig` command is used to tell your Cisco IronPort appliance where to look for service updates, including AsyncOS upgrades. By default, when you type the `upgrade` command, the appliance will contact Cisco IronPort's upgrade servers for the latest update. For remote upgrades, issue the `updateconfig` command and configure the appliance to use a local update server (the local server configured above).

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

```
Service (images):                Update URL:
-----
Feature Key updates              http://downloads.ironport.com/asyncos
Timezone rules                  IronPort Servers
IronPort AsyncOS upgrades       IronPort Servers

Service (list):                  Update URL:
-----
Timezone rules                  IronPort Servers
IronPort AsyncOS upgrades       IronPort Servers

Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled

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

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

| Service (images):   | Update URL:                          |
|---------------------|--------------------------------------|
| -----               |                                      |
| Feature Key updates | http://downloads.ironport.com/asynco |

1. Use Cisco IronPort update servers (http://downloads.ironport.com)
  2. Use own server
- [1]> **2**

Enter the HTTP base URL of the update server using the format (http://optionalname:password@local.server:port/directory/). The default HTTP port is 80; you do not need to specify the port unless you wish to use a non-standard port. The optional username/password will be presented using HTTP BASIC\_AUTH.  
[http://downloads.ironport.com/]>enter URL of the local server here



#### Note

You can use the `ping` command to ensure that the appliance can contact the local server. You can also use the `telnet` command to telnet to port 80 of the local server to ensure the local server is listening on that port.

## The upgrade Command

Issue the `upgrade` command to show a list of available upgrades. Select the desired upgrade from the list to install it. You may be asked to confirm messages or read and agree to license agreements.

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

```
Would you like to save the current configuration to the configuration
directory before upgrading? [Y]> y
```

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

```
Email a copy? [N]> y
```

```
Enter email addresses. Separate multiple addresses with commas.
[]> admin@example.com
```

```
Upgrades available.
```

1. AsyncOS 7.7.0 For Security Management upgrade



```
[1]> 1
```

```
Performing an upgrade may require a reboot of the system after the
upgrade is applied. You may log in again after this is done. Do you
wish to proceed with the upgrade? [Y]> y
```

```
Preserving configuration ...
Finished preserving configuration
IronPort Security Management Appliance(tm) Upgrade
Finding partitions... done.
Setting next boot partition to current partition as a precaution...
done.
Erasing new boot partition... done.
Installing application... done.
Installing CASE... done.
Installing Sophos Anti-Virus... done.
Reinstalling AsyncOS... done.
Installing Scanners... done.
Installing Brightmail Anti-Spam... done.
Installing Tracking Tools... done.
Configuring AsyncOS disk partitions... done.
Configuring AsyncOS user passwords... done.
Configuring AsyncOS network interfaces... done.
Configuring AsyncOS timezone... done.
Moving new directories across partitions... done.
Syncing... done.
Reinstalling boot blocks... done.
Will now boot off new boot partition... done.

Upgrade complete. It will be in effect after this mandatory reboot.

Upgrade installation finished.
Enter the number of seconds to wait before forcibly closing
connections.
[30]>
```

```
System rebooting. Please wait while the queue is being closed.
```

## Differences Between Upgrading Methods (Remote vs Streaming)

Note these differences when upgrading AsyncOS from a local server (Remote upgrade) as opposed to the traditional (Streaming upgrade) method:

- The upgrading installs immediately *while downloading*.

- A banner appears for 10 seconds at the beginning of the upgrade process. While this banner appears, you have the option to press Control-C to exit the upgrade process before downloading starts.

## Configuring Upgrade and Service Update Settings

You can configure how the Security Management appliance downloads security services updates, such as time zone rules and AsyncOS upgrades. For example, you can choose which network interface to use when downloading the files, configure the update interval, or disable automatic updates.

AsyncOS periodically queries the update servers for new updates to all security service components except for new AsyncOS upgrades. To upgrade AsyncOS, you must manually prompt AsyncOS to query for available upgrades.

You can configure upgrade and updates settings on the Management Appliance > System Administration > Update Settings page in the GUI or using the `updateconfig` command in the CLI.

You can also upgrade the Cisco IronPort AsyncOS using the Update Settings page or the `updateconfig` CLI command. For more information, see [Upgrading AsyncOS, page 12-17](#).



### Note

The Cisco IronPort AsyncOS update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for AsyncOS upgrades. If you determine that your firewall settings require a static IP address for updates, follow instructions below for editing the update settings and contact Cisco IronPort Customer support to obtain the required URL addresses.

## Editing Update Settings

To edit the update settings for your Cisco IronPort appliance, click the **Edit Update Settings** button to display the Edit Update Settings page.

[Table 12-1](#) describes the update and upgrade settings you can configure.

**Table 12-1**      ***Update Settings for Security Services***

| Setting                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Update Servers (images)</b> | <p>Choose whether to download Cisco IronPort AsyncOS upgrade images and service updates, such as time zone rules, from the Cisco IronPort update servers or a local web server. The default is the Cisco IronPort update servers.</p> <p>You might want to choose a local web server under either of the following circumstances:</p> <ul style="list-style-type: none"> <li>• You want to download the upgrade and update images from Cisco IronPort, but you need to enter a static address provided by Cisco IronPort Customer Support.</li> <li>• You want to temporarily download an upgrade image stored on a local web server. After you download the image, Cisco IronPort recommends changing this setting back to the Cisco IronPort update servers (or the static address if you used that) so that security components continue to update automatically.</li> </ul> <p>When you choose a local update server, enter the base URL and port number for the servers used to download the upgrades and updates. If the server requires authentication, you can also enter a valid user name and password.</p> |
| <b>Update Servers (lists)</b>  | <p>Choose whether to download the list of available upgrades and security service updates (the manifest XML file) from the Cisco IronPort update servers or a local web server.</p> <p>The default is the Cisco IronPort update servers. You might want to choose a local web server when you want to temporarily download an upgrade image stored on a local web server. After you download the image, Cisco IronPort recommends changing this setting back to the Cisco IronPort update servers so that security components continue to update automatically.</p> <p>When you choose a local update server, enter the full path to the manifest XML file for the list including the file name and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and password.</p> <p>For more information, see <a href="#">Remote vs. Streaming Upgrades, page 12-18</a> and <a href="#">Remote Upgrade Overview, page 12-20</a>.</p>                                                                            |

**Table 12-1**      *Update Settings for Security Services (continued)*

| Setting            | Description                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Automatic Updates  | Choose whether or not to enable automatic updates for the listed security updates, such as time zone rules. When enabled, enter the time to wait between checks for updates. Add a trailing <b>m</b> for minutes, <b>h</b> for hours, and <b>d</b> for days.  |
| Interface          | Choose which network interface to use when contacting the update servers for the listed security component updates and Cisco IronPort AsyncOS upgrades. The available proxy data interfaces are shown. By default, the appliance selects an interface to use. |
| HTTP Proxy Server  | If an upstream HTTP proxy server exists and requires authentication, enter the server information and user name and password here.<br><br>Note that if you specify a proxy server, it will be used to access and update the services listed in the GUI.       |
| HTTPS Proxy Server | If an upstream HTTPS proxy server exists and requires authentication, enter the server information and user name and password here.<br><br>Note that if you specify a proxy server, it will be used to access and update the services listed in the GUI.      |

## Configuring the Update and Upgrade Settings from the GUI

To edit the AsyncOS update and upgrade settings:

- Step 1

Navigate to the Management Appliance > System Administration > Update Settings page, and click **Edit Update Settings**. The Edit Update Settings page is displayed.

Figure 12-8 shows the options you can configure on the Edit Update Settings page.

**Figure 12-8 Edit Update Settings Page****Edit Update Settings**

| Update Settings for Security Services |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Update Servers (images):              | <p>The update servers will be used to obtain <b>update images</b> for the following services:</p> <ul style="list-style-type: none"> <li>- Feature Key updates</li> <li>- Time zone rules</li> <li>- IronPort AsyncOS upgrades</li> </ul> <p><input checked="" type="radio"/> IronPort Update Servers</p> <p><input type="radio"/> Local Update Servers (location of update image files)</p> <p>Base Url (all services except Time zone rules and IronPort AsyncOS upgrades): <input type="text" value="http://downloads.ironport.com/"/> Port: <input type="text" value="80"/><br/> <input type="text" value="http://downloads.example.com"/></p> <p>Authentication (optional):</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Retype Password: <input type="text"/></p> <p>Base Url (Time zone rules and IronPort AsyncOS upgrades): <input type="text" value=""/><br/> format: downloads.example.com:80</p> |
| Update Servers (list):                | <p>The URL will be used to obtain the <b>list of available updates</b> for the following services:</p> <ul style="list-style-type: none"> <li>- Time zone rules</li> <li>- IronPort AsyncOS upgrades</li> </ul> <p><input checked="" type="radio"/> IronPort Update Servers</p> <p><input type="radio"/> Local Update Servers (location of list of available updates file)</p> <p>Full Url: <input type="text" value="http://updates.example.com/my_updates.xml"/><br/> <input type="text" value="http://updates.example.com/my_updates.xml"/> Port: <input type="text" value="80"/></p> <p>Authentication (optional):</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Retype Password: <input type="text"/></p>                                                                                                                                                                                                |
| Automatic Updates:                    | <p><input checked="" type="checkbox"/> Enable automatic updates for Time zone rules</p> <p>Update Interval: <input type="text" value="5m"/></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Interface:                            | <p><input type="text" value="Auto Select"/> <input type="button" value="v"/></p> <p>Interface section applies only to Time zone rules and IronPort AsyncOS upgrades</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Proxy Servers (optional):             | <p><b>HTTP Proxy Server</b></p> <p>If an HTTP proxy server is defined it will be used to update the following services:</p> <ul style="list-style-type: none"> <li>- Feature Key updates</li> <li>- Time zone rules</li> <li>- IronPort AsyncOS upgrades</li> </ul> <p>HTTP Proxy Name: <input type="text"/> Port: <input type="text" value="80"/></p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Retype Password: <input type="text"/></p> <p><b>HTTPS Proxy Server</b></p> <p>If an HTTPS proxy server is defined it will be used to update the following services:</p> <ul style="list-style-type: none"> <li>- Time zone rules</li> <li>- IronPort AsyncOS upgrades</li> </ul> <p>HTTPS Proxy Name: <input type="text"/> Port: <input type="text" value="80"/></p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Retype Password: <input type="text"/></p>                |

**Step 2** Configure the settings in [Table 12-1 on page 12-33](#).

**Step 3** Submit and commit your changes.

# Disaster Recovery on the Security Management Appliance

Disaster recovery allows you to prepare for a situation when the Security Management appliance might suddenly fail. Failure management and disaster recovery during these times is crucial to the wellbeing of your data. In these cases it is important to know how to implement and recover data so that your system can retain data integrity.

**Note**

---

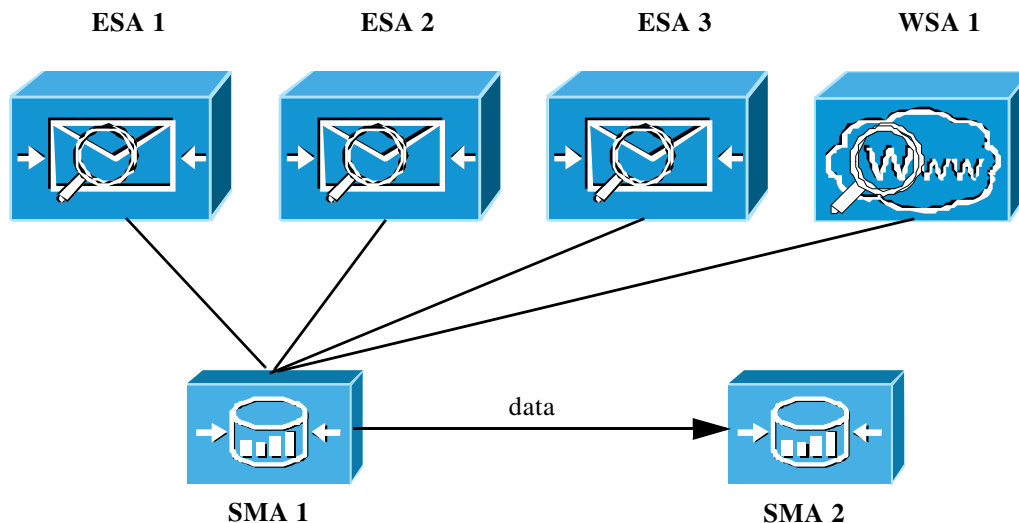
It is important to remember that while it is possible to transfer data between Security Management appliances that are different sizes, the appliance that you are transferring data to must have the same size allocations or greater.

Even with this recommendation, there is no strict rule that does not allow you to perform disaster recovery and backup from a larger to a smaller Security Management appliance. You can schedule a backup from source to target Security Management appliance as long as there is enough space on the target for all of the data being backed up. That is, the disk quota allocated for all of your data on the target appliance should not be less than that on the source appliance.

For example, if you have a larger appliance, the M1060, as source and a smaller appliance, the M650 as target, be sure to reduce the space allocated on the larger M1060 for all of the data, so that the numbers match with the space that you have on the smaller M650 appliance. This can be accomplished from the Disk Management page on the GUI. Additionally, make sure that you do not have more data on the larger M1060 than the smaller M650 can accommodate.

---

To get started, let's take a look at a typical environment and configuration. In a typical environment, your appliance configuration may look like the following configuration in [Figure 12-9](#):

**Figure 12-9 Disaster Recovery: A Typical Environment**

In this environment, SMA 1 is the primary Security Management appliance that is receiving email reporting, tracking, ISQ, and Web reporting data from ESA 1-3 and WSA 1. After data is received by SMA 2, a backup is performed on SMA 1 to make sure that all data on SMA 1 is copied and stored on SMA 2 for failover purposes. See [Backing Up Your Security Management Appliance, page 12-8](#) for information on backing up your Security Management appliance.

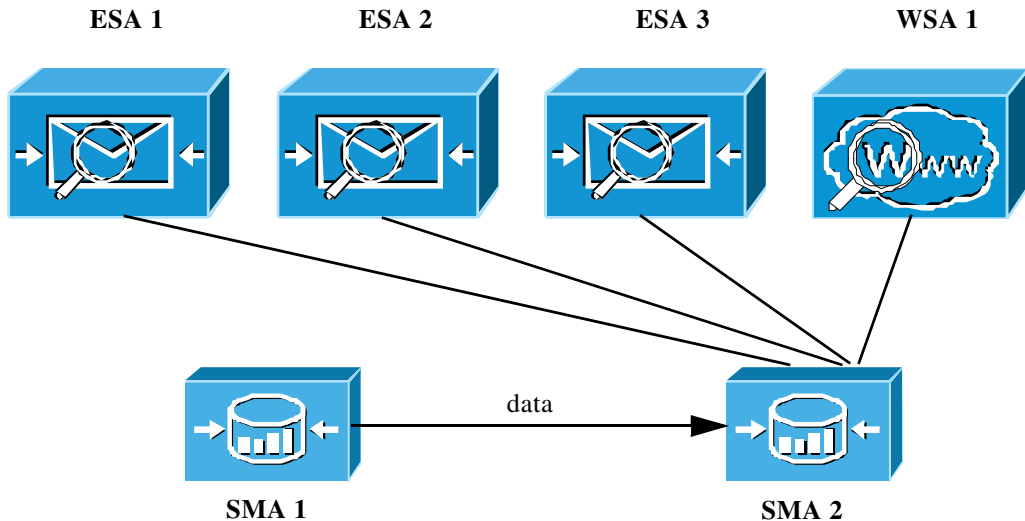
Now, let's assume that you detect that SMA 1 is starting to fail. Reports are coming in slowly, data is being corrupted, or there is some indication that the Security Management appliance is beginning to fail. Follow the steps below to initiate disaster recovery.

---

**Step 1** Start an instant backup of SMA1 to SMA 2.

See [Immediate Backups, page 12-14](#) for the steps on how to perform this step.

After the backup is performed, your environment configuration now looks like the diagram in [Figure 12-10](#).

**Figure 12-10 Disaster Recovery: Part 1—Instant Backup**

All data is instantly transferred over from SMA 1 to SMA 2. Additionally, all data from ESA 1-3 and WSA 1 now goes to SMA 2. SMA 2 now becomes the primary appliance. At this point you must manually configure SMA 2.

- Step 2** Recreate the IP address from the failed SMA 1 to be the IP address on SMA 2:
- On SMA 2 choose **Network > IP Interfaces > Add IP Interfaces**.
  - On the **Add IP Interfaces** page, enter all of the relevant IP Interface information from the failed SMA1 into the text fields to recreate the interface on SMA 2.
- For more information on Adding IP Interfaces, see [Configuring IP Interfaces, page A-2](#).
- Step 3** Click **Submit** and **Commit**.
- Step 4** Add all appliances on to the new Security Management appliance (SMA 2).  
For information on how to add appliances, see [Adding Managed Appliances, page 3-10](#).
- Step 5** Enable all of the services on the new Security Management appliance (SMA 2).

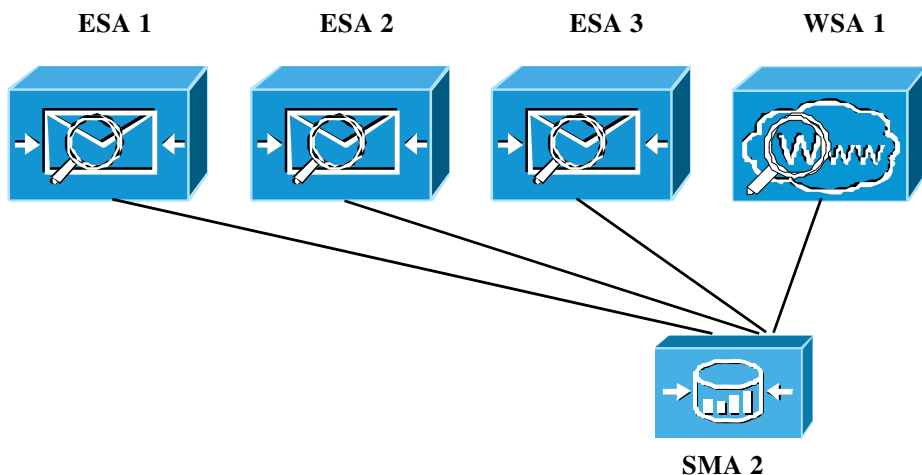


In this case, you must re-enable services for ESA 1-3 and WSA 1. For more information on enabling services, see [Enabling Services on the Security Management Appliance, page 3-2](#).

**Step 6** Test to see that each appliance is enabled and working by establishing a connection to the appliances and testing the connections.

At this point you have all data directed to SMA 2 as shown in [Figure 12-11](#).

**Figure 12-11** *Disaster Recovery: Part 2—New Security Management Appliance*



**Note**

If you have periodically saved your configuration using the **saveconfig** command, you can load this saved configuration file to the new Security Management appliance (SMA 2 in this example) by using the **loadconfig** command and then setting the new IP address described in Step 2. The configuration file does not include all information needed to make the SMA 2 function. You will still need to add all of the appliances to the new Security Management appliance. From there, you must establish a connection to each appliance and test the connections.

# About Distributing Administrative Tasks

You can distribute administrative tasks to other people based on the user roles that you assign to their user accounts.

The Security Management appliance offers both predefined and custom user roles for monitoring and managing your email and web security appliances.

For descriptions of the predefined roles, see [User Roles, page 12-40](#).

For more information about custom user roles, see [Delegating Administration with Custom User Roles, page 12-45](#).

For information about user accounts, see [Managing Users with the GUI, page 12-55](#).

## User Roles

Except as noted, you can assign each user a predefined user role with the privileges described in the following table, or a custom user role.

**Table 12-2**      *Descriptions of User Roles*

| User Role Name | Description                                                                                                                                                                                                                                                                                                                                                                             | Web Reporting/<br>Scheduled<br>Reports<br>Capability | Appliance                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------|
| admin          | The <b>admin</b> user is the default user account for the system and has all administrative privileges. The admin user account is listed here for convenience, but it cannot be assigned via a user role, and it cannot be edited or deleted, aside from changing the password.<br><br>Only the <b>admin</b> user can issue the <b>resetconfig</b> , <b>revert (ESA only)</b> commands. | Yes/Yes                                              | Security Management appliance |

**Table 12-2**      *Descriptions of User Roles*

| User Role Name       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Web Reporting/<br>Scheduled<br>Reports<br>Capability | Appliance                                                                             |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Administrator</b> | <p>User accounts with the Administrator role have full access to all configuration settings of the system.</p> <p>On the Email Security appliance, all features that were previously only available to <b>admin</b> user are now available to those that are assigned with the Administrator role.</p>                                                                                                                                                                                           | Yes/Yes                                              | Security Management appliance,<br>Web Security appliance<br>Email Security appliance  |
| <b>Operator</b>      | <p>User accounts with the Operator role are restricted from:</p> <ul style="list-style-type: none"> <li>• Creating or editing user accounts</li> <li>• Issuing the <code>resetconfig</code> command</li> <li>• Checking for available upgrades with the <code>upgradecheck</code> command</li> <li>• Installing upgrades with the <b>upgradeinstall</b> command</li> <li>• Running the System Setup Wizard</li> </ul> <p>Otherwise, they have the same privileges as the Administrator role.</p> | Yes/Yes                                              | Security Management appliance,<br>Web Security appliance,<br>Email Security appliance |
| <b>Technician</b>    | <p>User accounts with the Technician role can initiate system administration activities such as upgrades, reboots managing feature keys, and so forth. This role does not have access to email specific functions like policies, HAT or RAT.</p>                                                                                                                                                                                                                                                 | No/No                                                | Security Management appliance,<br>Web Security appliance<br>Email Security appliance  |

**Table 12-2**      *Descriptions of User Roles*

| <b>User Role Name</b>              | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                      | <b>Web Reporting/<br/>Scheduled<br/>Reports<br/>Capability</b> | <b>Appliance</b>                                                                |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>Read-Only Operator</b>          | 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, if access is enabled. Users with this role cannot access the file system, FTP, or SCP. | Yes/No                                                         | Security Management appliance, Web Security appliance, Email Security appliance |
| <b>Guest</b>                       | 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, if access is enabled. Users with the Guest role cannot access Message Tracking.                                                                                                                                                          | Yes/No                                                         | Security Management appliance, Web Security appliance, Email Security appliance |
| <b>Web Administrator</b>           | User accounts with the Web Administrator role have access to all configuration settings within the <b>User Roles</b> menu only.                                                                                                                                                                                                                                                                         | Yes/No                                                         | Security Management appliance                                                   |
| <b>Web Policy Administrator</b>    | User accounts with the Web Policy Administrator role can access the Web Appliance Status page and all pages in the Configuration Master. The web policy administrator can configure identities, access policies, decryption policies, routing policies, proxy bypass, custom URL categories, and time ranges. The web policy administrator cannot publish configurations.                               | No/No                                                          | Security Management appliance                                                   |
| <b>URL Filtering Administrator</b> | User accounts with the URL Filtering Administrator role can configure URL filtering only.                                                                                                                                                                                                                                                                                                               | No/No                                                          | Security Management appliance                                                   |

**Table 12-2**      *Descriptions of User Roles*

| <b>User Role Name</b>      | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                             | <b>Web Reporting/<br/>Scheduled<br/>Reports<br/>Capability</b> | <b>Appliance</b>                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------|
| <b>Email Administrator</b> | User accounts with the Email Administrator role have access to all configuration settings within the Email menu only, including Cisco IronPort Spam Quarantine and system quarantine rights.                                                                                                                                                                                                   | No/No                                                          | Security Management appliance                           |
| <b>Help Desk User</b>      | <p>User accounts with the Help Desk User role are restricted to:</p> <ul style="list-style-type: none"><li>• Message Tracking</li><li>• Managing the Cisco IronPort Spam Quarantine</li></ul> <p>Users with this role cannot access the rest of the system, including the CLI. You need to enable access to the Cisco IronPort Spam Quarantine before a user with this role can manage it.</p> | No/No                                                          | Security Management appliance, Email Security appliance |

Table 12-2 Descriptions of User Roles

| User Role Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Web Reporting/<br>Scheduled<br>Reports<br>Capability | Appliance                                               |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|---------------------------------------------------------|
| Custom Roles   | <p>User accounts that are assigned a custom user role can view and configure only policies, features, or specific policy or feature instances that have been specifically delegated to the role.</p> <p>You can create a new Custom Email User Role or a new Custom Web User Role from the Add Local User page. However, you must assign privileges to this Custom User Role before the role can be used. To assign privileges, go to Management Appliance &gt; System Administration &gt; User Roles and click the user name.</p> <p><b>Note</b> Users assigned to a Custom Email User Role cannot access the CLI.</p> <p>For more information, see <a href="#">Delegating Administration with Custom User Roles, page 12-45</a>.</p> | No/No                                                | Security Management appliance, Email Security appliance |

Some roles can access both the GUI and the CLI: Administrator, Operator, Guest, Technician, and Read-Only Operator. Other roles can access the GUI only: Help Desk User, Email Administrator, Web Administrator, Web Policy Administrator, URL Filtering Administrator, and custom user.

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 12-66](#).

Before users can access the Spam Quarantine, you must enable that access. See [Configuring Administrative Users for Cisco IronPort Spam Quarantine, page 7-6](#).

## Delegating Administration with Custom User Roles

The Security Management appliance allows users with Administration privileges to delegate administration capabilities to custom roles. Custom roles provide more flexible control over your users' access than the predefined user roles do.

Users to whom you assign custom user roles can manage policies or access reports for a subset of appliances, features, or end users. For example, you might allow a delegated administrator for web services to manage policies for an organization's branch office in a different country, where the acceptable use policies might be different from those at the organization's headquarters. You delegate administration by creating custom user roles and assigning access permissions to those roles. You determine which policies, features, reports, custom URL categories, etc. that the delegated administrators can view and edit.

For more information, see:

- [About Custom Email User Roles, page 12-45](#)
- [About Custom Web User Roles, page 12-51](#)

## About Custom Email User Roles

You can assign custom roles to allow delegated administrators to access the following on the Security Management appliance:

- All reports (optionally restricted by Reporting Group)
- Mail Policy reports (optionally restricted by Reporting Group)
- DLP reports (optionally restricted by Reporting Group)
- Message Tracking
- Spam Quarantine

Detailed information about each of these items follows this section. In addition, all users granted any of these privileges can see the System Status, available under the Management Appliance tab > Centralized Services menu. Users assigned to custom email user roles cannot access the CLI.

**Note**

You can also create custom user roles directly on each Email Security appliance. Custom user roles on the Email Security appliance offer access to functions that are not available to custom user roles on the Security Management appliance. For example, you can delegate access to mail and DLP policies and content filters. For details, see the “Managing Custom User Roles for Delegated Administration” section in the “Common Administration” chapter of the *Cisco IronPort AsyncOS for Email Daily Management Guide*.

## Email Reporting

You can grant custom user roles access to Email reports as described in the following sections.

For complete information about the Email Security Monitor pages on the Security Management appliance, see the chapter on [Using Centralized Email Reporting](#).

### All Reports

If you grant a custom role access to All Reports, users assigned to this role can see the following Email Security Monitor pages either for all Email Security appliances, or for the Reporting Group that you select:

- Overview
- Incoming Mail
- Outgoing Destinations
- Outgoing Senders
- Internal Users
- DLP Incidents
- Content Filters
- Virus Types
- TLS Connections
- Outbreak Filters
- System Capacity
- Reporting Data Availability
- Scheduled Reports



- Archived Reports

### **Mail Policy Reports**

If you grant a custom role access to Mail Policy Reports, users assigned to this role can see the following Email Security Monitor pages either for all Email Security appliances, or for the Reporting Group that you select:

- Overview
- Incoming Mail
- Outgoing Destinations
- Outgoing Senders
- Internal Users
- Content Filters
- Virus Types
- Outbreak Filters
- Reporting Data Availability
- Archived Reports

### **DLP Reports**

If you grant a custom role access to DLP Reports, users assigned to this role can see the following Email Security Monitor pages either for all Email Security appliances, or for the Reporting Group that you select:

- DLP Incidents
- Reporting Data Availability
- Archived Reports

## **Message Tracking**

If you grant a custom role access to Message Tracking, users to whom you assign this role can find the status of all messages tracked by the Security Management appliance.

To control access to sensitive information in messages that violate DLP policies, see [Disabling Access to Sensitive Information in Message Tracking, page 12-59](#).

For more information about message tracking, including instructions for setting up your appliances to enable access to message tracking on the Security Management appliance, see [“Tracking Email Messages”](#).

## Quarantines

If you grant a custom role access to Quarantines, users to whom you assign this role can search for, view, deliver, or delete messages in the Spam Quarantine on this Security Management appliance.

Before users can access the Spam Quarantine, you must enable that access. See [Configuring Administrative Users for Cisco IronPort Spam Quarantine, page 7-6](#).

For complete information about the Spam Quarantine, including instructions for setting up your appliances to enable access to this quarantine from the Security Management appliance, see the [“Managing the Cisco IronPort Spam Quarantine”](#) chapter.

## Creating Custom Email User Roles

You can create custom email user roles for access to Email Reporting, Message Tracking, and the Spam Quarantine.

For descriptions of the access that each of these options permits, see [About Custom Email User Roles](#) and its subsections.



### Note

To grant more granular access or access to other features, reports, or policies, create custom user roles directly on each Email Security appliance.

**Step 1** On the main Security Management appliance, choose **Management Appliance > System Administration > User Roles**.

The User Roles page appears.

**Step 2** Click **Add Email User Role**.



### Tip

Alternatively, you can create a new role by duplicating an existing Email User Role: Click the Duplicate icon in the applicable table row, then modify the resulting copy.

The Add Email User Role page appears.

**Figure 12-12 Add Email User Role Page**

### Add Email User Role

| Settings           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name:              | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Description:       | <div></div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Access Privileges: | <div> Email Reporting: <input checked="" type="radio"/> No Access <input type="radio"/> Access to data by Reporting Group <div>All Reports</div> <input type="radio"/> Access to data from all Email Appliances <div>All Reports</div> </div> <div> Message Tracking: <input checked="" type="radio"/> No Access <input type="radio"/> View Message Tracking </div> <div> Quarantines: <input checked="" type="radio"/> No Access <input type="radio"/> Spam Quarantine Access </div> |

Cancel

Submit

- Step 3** Enter a unique name for the user role (for example, “dlp-auditor”) and a description. Email and Web custom user role names must not be duplicated.



**Note** The name must contain only lowercase letters, numbers, and dashes. It cannot start with a dash or a number.

- Step 4** Choose the access privileges to enable for this role.
- Step 5** Click **Submit** to return to the User Roles page, which lists the new user role.
- Step 6** If you limited access by Reporting Group, click the **no groups selected** link in the Email Reporting column for the user role, then choose at least one Reporting Group.
- Step 7** Commit your changes.

- Step 8** If you granted this role access to spam quarantine, enable access for this role. See [Configuring Administrative Users for Cisco IronPort Spam Quarantine, page 7-6](#).
- 

## Editing Custom Email User Roles

- 
- Step 1** On the User Roles page, click the role name to display the Edit Email User Role page.
- Step 2** Edit any of the settings.
- Step 3** Submit and commit your changes.
- Step 4** If you granted this role access to spam quarantine, enable access for this role. See [Configuring Administrative Users for Cisco IronPort Spam Quarantine, page 7-6](#).
- 

## Using Custom Email User Roles

When a user who is assigned a custom email user role logs into the appliance, that user sees only the links to the security features to which that user has access. The user can return to this main page at any time by selecting Account Privileges in the Options menu. These users can also access the features to which they have access by using the menus at the top of the web page. In the following example, the user has access to all features that are available on the Security Management appliance via custom email user roles.

**Figure 12-13** Account Privileges Page for a Delegated Administrator assigned Custom Email User Roles

Logged in as: **full-access** on **example.com**  
Options ▾ Help and Support

### Account Privileges (full-access)

|                  |                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------|
| Email Reporting  | <a href="#">Mail Policy Reports from all Email Appliances</a><br><i>View and analyze email traffic.</i>   |
| Message Tracking | <a href="#">Message Tracking</a><br><i>Track messages.</i>                                                |
| Quarantines      | <a href="#">Manage messages in the Spam Quarantine</a><br><i>Manage messages in assigned Quarantines.</i> |

## About Custom Web User Roles

Custom web user roles allow users to publish policies to different Web Security appliances, and gives them the permission to edit or publish the custom configuration to different appliances.

From the **Web > Configuration Master > Custom URL Categories** page on the Security Management appliance, you can view the URL categories and policies that you are allowed to administer and publish. Additionally, you can go to the **Web > Utilities > Publish Configuration Now** page and view the possible configurations.



#### Note

Remember that when you create a custom role with Publish Privilege capabilities, when user logs in, they will not have any usable menus. They do not have the publish menu and they will land on an non-editable landing screen since the URL and policy tabs do not have any capabilities. In effect, you have a user that cannot publish or administer any categories or policies .

The workaround to this issue is that if you want a user to be able to publish, but not to be able to manage any categories or policies, you **must** create a custom category which is not used in any policy, and give that user the ability to manage that custom category along with publishing. In this way, if they add or delete URLs from that category, it does not affect anything.

---

You can delegate web administration by creating and editing custom user roles.

- [Creating Custom Web User Roles](#)
- [Editing Custom Web User Roles](#)

## Creating Custom Web User Roles

To create a custom web user role, perform the following steps:

- 
- Step 1** On the main Security Management appliance, choose **Management Appliance > System Administration > User Roles**.

The User Roles page appears.

- Step 2** Click **Add Web User Role**.



**Tip**

Alternatively, you can create a new role by duplicating an existing Web User Role: Click the Duplicate icon in the applicable table row, then modify the resulting copy.

---

The Add Web User Role page appears.

**Figure 12-14 Add Web User Role Page****Add Web User Role**

| Settings                               |                                                                                                |
|----------------------------------------|------------------------------------------------------------------------------------------------|
| Name:                                  | <input type="text"/>                                                                           |
| Description:                           | <input type="text"/>                                                                           |
| Visibility of Policies and Categories: | <input checked="" type="radio"/> Visible by default<br><input type="radio"/> Hidden by default |
| Publish Privilege: (?)                 | <input checked="" type="radio"/> Off<br><input type="radio"/> On                               |

- Step 3** Enter a unique name for the user role (for example, “canadian-admins”) and a description.



**Note** The name must contain only lowercase letters, numbers, and dashes. It cannot start with a dash.

- Step 4** Choose whether you want the policies and custom URL categories to be visible or hidden by default.

- Step 5** Choose whether you want Publish privileges turned on or off.

This privilege allows the user to publish any Configuration Master for which the user can edit Access Policies or URL Categories.

- Step 6** Choose whether to start with new (empty) settings or to copy an existing custom user role. If you choose to copy an existing user role, choose from the list the role that you want to copy.

- Step 7** Click **Submit** to return to the User Roles page, which lists the new user role.



**Note** If you have enabled the anonymized feature within web reporting, all user roles with access to web reporting will have unrecognizable user names and roles in the interactive reports page. See the [Managing Scheduled Reports](#) section in [Chapter 5, “Using Centralized Web Reporting.”](#) The exception is the Administrator role, which is able to see actual user names in the scheduled reports. If the anonymize feature is enabled, scheduled reports that are generated by the Operator and Web Administrator are anonymized.

Figure 12-15 User Roles Page

| Web Roles            |                                                |                                                |             |                |                                                                                     |                                                                                     |
|----------------------|------------------------------------------------|------------------------------------------------|-------------|----------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Add Web User Role... |                                                |                                                |             |                |                                                                                     |                                                                                     |
| Role Name            | Privileges                                     |                                                | Description | Assigned Users | Duplicate                                                                           | Delete                                                                              |
|                      | Configuration Master 5.7.1                     | Configuration Master 6.3.0                     |             |                |                                                                                     |                                                                                     |
| canadian admins      | Access Policies: 0<br>Custom URL Categories: 0 | Access Policies: 0<br>Custom URL Categories: 0 |             |                |  |  |



**Note** If you use the **Web > Utilities > Security Services Display > Edit Security Services Display** page to hide one of the Configuration Masters, the User Roles page also hides the corresponding Configuration Master column; however, privilege settings for the hidden Configuration Master are retained.

## Editing Custom Web User Roles

To edit settings for a custom web user role:

- Step 1

On the User Roles page, click the role name to display the Edit User Role page.
- Step 2

Edit any of the settings: name, description, and visibility of policies and custom URL categories.
- Step 3

Click **Submit**.

To edit privileges for a custom user role:

Navigate to the User Roles page.

- To edit access policy privileges, click “Access policies” to display a list of access policies configured in the Configuration Master. In the Include column, select the check boxes of the policies to which you want to give the user edit access. Click **Submit** to return to the User Roles page.

-or-



- To edit custom URL category privileges, click Custom URL Categories to display a list of the custom URL categories defined on the Configuration Master. In the Include column, select the check boxes of the custom URL categories to which you want to give the user edit access. Click **Submit** to return to the User Roles page.
- 

## Managing Users with the GUI

You will use user accounts to assign user roles for performing administrative tasks.

The Cisco IronPort appliance provides two methods for adding user accounts: creating user accounts on the appliances themselves, 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 **Management Appliance > 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 12-66](#).

There is no limit to the number of user accounts that you can create on the appliance.

To manage user accounts:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > Users**.

The Users page appears.

Figure 12-16 Users Page

Users

Add User...

| <div>All</div> <div>Accounts</div> | User Name       | Full Name                  | User Role                        | Account Status | Password Expires | Delete |
|------------------------------------|-----------------|----------------------------|----------------------------------|----------------|------------------|--------|
| <input type="checkbox"/>           | 1-helpdesk      | predefined helpdesk privs  | Help Desk User                   | Active         | n/a              |        |
| <input type="checkbox"/>           | 2-operator-ro   | read only operator         | Read-Only Operator               | Active         | n/a              |        |
| <input type="checkbox"/>           | 3-guest         | guest privs                | Guest                            | Active         | n/a              |        |
| <input type="checkbox"/>           | 4-e-admin       | email administrator        | Email Administrator              | Active         | n/a              |        |
| <input type="checkbox"/>           | 5-operator      | operator                   | Operator                         | Active         | n/a              |        |
| <input type="checkbox"/>           | full-access     | Full Access                | full access*                     | Active         | n/a              |        |
| <input type="checkbox"/>           | msg-trackg      | msg trackg                 | message tracking only*           | Active         | n/a              |        |
| <input type="checkbox"/>           | nemailrole      | new custom email user role | new custom email user role*      | Active         | n/a              |        |
| <input type="checkbox"/>           | new-operator    | new operator               | Operator                         | Active         | n/a              |        |
| <input type="checkbox"/>           | no-privs        | custom with no privs       | no-privs*                        | Active         | n/a              |        |
| <input type="checkbox"/>           | pre-admin       | predefined Admin role      | Administrator                    | Active         | n/a              |        |
| <input type="checkbox"/>           | quarantine      | quarantine access          | quarantines only*                | Active         | n/a              |        |
| <input type="checkbox"/>           | reportg-all     | reporting - all appliances | reporting only - all appliances* | Active         | n/a              |        |
| <input type="checkbox"/>           | reportg-mpolicy | reporting - mail policy    | reporting - mail policy*         | Active         | n/a              |        |
| <input type="checkbox"/>           | reporting-dlp   | reporting dlp              | reporting - DLP*                 | 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 administrative users for the system, including the user name, full name, and user role. The Users page also indicates whether external authentication is enabled, and the authentication type.



Note

Asterisks indicate users assigned custom user roles for delegated administration. “Unassigned” appears in red if the user’s custom role has been deleted. For more information on user roles, including descriptions, see [User Roles, page 12-40](#).

From the Users page, you can:

- Add new users.

- Delete users.
- Edit users (including changing the admin user's password).
- Edit external authentication settings.

## Adding Users

Follow this procedure to add users directly to the Security Management appliance if you are not using external authentication.

- 
- Step 1** If you will assign custom user roles, we recommend that you define those roles first. See [Delegating Administration with Custom User Roles](#), page 12-45.
- Step 2** On the Security Management appliance, choose **Management Appliance > System Administration > Users**.
- Step 3** Click **Add User**.  
The Add Local User page appears.

**Figure 12-17 Adding a User**

### Add Local User

| Local User Settings |                                                                                                                                                                                                                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account Status:     | Active                                                                                                                                                                                                                                                                                                  |
| User Name:          | <input type="text"/>                                                                                                                                                                                                                                                                                    |
| Full Name:          | <input type="text"/>                                                                                                                                                                                                                                                                                    |
| User Role: ?        | <div> <input type="radio"/> Predefined Roles           <div> <input type="text" value="Administrator"/> </div> </div> <div> <input checked="" type="radio"/> Custom Roles           <div> <div> Add Email Role...<br/> Add Web Role... </div> <input type="text" value="New Role Name:"/> </div> </div> |
| Password:           | <div> <input type="text"/> </div> <div> <input type="text"/> </div> <div> A password must contain the following: <ul style="list-style-type: none"> <li>at least 6 characters.</li> </ul> </div>                                                                                                        |

- Step 4** Enter a unique name for the user. You cannot enter words that are reserved by the system (such as “operator” and “root”).
- Step 5** Enter a full name for the user.

- Step 6** Select a predefined role or a custom role. See [Table 12-2](#) for more information about user roles.
- If you add a new Email role or Web role here, enter a name for the role. For naming restrictions, see [Creating Custom Email User Roles, page 12-48](#) or [Creating Custom Web User Roles, page 12-52](#).
- Step 7** Enter a password and reenter it. Passwords must be at least six characters long.
- Step 8** Click **Submit** to add the user.
- Step 9** Click **Commit** to commit your changes.
- Step 10** If you added a custom user role on this page, assign privileges to that role now. See [Delegating Administration with Custom User Roles, page 12-45](#).
- 

## Editing Users

To edit a user (for example, to change a password):

- 
- Step 1** Click the user's name in the Users listing. The Edit Local User page appears.
- Step 2** Make changes to the user.
- Step 3** Click **Submit** and then click **Commit** to commit your changes.
- 

## Deleting Users

To delete a user:

- 
- Step 1** Click the trash can icon corresponding to the user's name in the Users listing.
- Step 2** Confirm the deletion by clicking **Delete** in the warning dialog that appears.
- Step 3** Click **Commit** to commit your changes.
-

## Disabling 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 non-Administrator users who have access to Message Tracking. Administrator users can always see this content.

To hide sensitive content from non-Administrator users:

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

**Figure 12-18** *DLP Tracking Privileges Page*  
**DLP Tracking Privileges**

DLP Tracking Privileges

This setting applies to non-Administrator accounts of either local or external authentication account types.

DLP Tracking Privileges: ? ☒ Allow access to DLP Matched Content in Message Tracking results.

Cancel Submit

- Step 3** Deselect the **Allow access to DLP Matched Content in Message Tracking results** check box.
- Step 4** Submit and commit your changes.

The Centralized Email Message Tracking feature must be enabled under Management Appliance > Centralized Services for this setting to take effect.

---

## Additional Commands to Support Multiple Users: who, whoami, and last

The following commands support multiuser access to the appliance.

- The **who** command lists all users who are logged in to 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 user name 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 also appear.

```
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 Management Appliance > System Administration > Users page in the Local User Account and Password Settings section.

[Figure 12-19](#) shows the Local User Account and Password Settings section on the Users page.

**Figure 12-19 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. |
| <a href="#">Edit Settings...</a>       |                                |

To configure user account and password restrictions:

- Step 1** On the Management Appliance > 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 12-20 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.*<br><input type="checkbox"/> Display Locked Account Message<br><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><i>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.</i></p> |
| Password Reset:                                     | <input type="checkbox"/> Require a password reset whenever a user's password is set or changed by an admin (Recommended).<br><input type="checkbox"/> Require users to reset passwords after <input type="text" value="90"/> days.<br><div style="margin-left: 20px;"> <input type="checkbox"/> Display reminder <input type="text" value="14"/> days before expiration.                 </div>                                                                                                                                                                                                     |
| Password Rules:                                     | Require at least <input type="text" value="6"/> characters.<br><input type="checkbox"/> Require at least one upper (A-Z) and one lower (a-z) case letter.<br><input type="checkbox"/> Require at least one number (0-9).<br><input type="checkbox"/> Require at least one special character. (?)<br><input type="checkbox"/> Ban usernames and their variations as passwords.<br><input type="checkbox"/> Ban reuse of the last <input type="text" value="3"/> passwords.                                                                                                                           |
| <p><i>*Settings do not apply to Admin User.</i></p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



**Step 2** Configure the settings described in [Table 12-3](#).

**Table 12-3** *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 a locked account.</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><b>Note</b> You can also manually lock individual user accounts.</p> |

**Table 12-3**      **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 uses.</p> <p>After a password expires, the user is forced to change the account password at the next login.</p> <p><b>Note</b>      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.</p> |
| Password Rules:<br>Require at <number><br>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:<br>Require at least one<br>number (0-9).    | <p>Choose whether or not the passwords must contain at least one number.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 12-3 Local User Account and Password Settings (continued)**

| Setting                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password Rules:<br>Require at least one special character.          | Choose whether or not the passwords must contain at least one special character. Passwords may contain the following special characters:<br>~ ? ! @ # \$ % ^ & * - _ + =<br>\   / [ ] ( ) < > { } ` ' " ; : , .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Password Rules:<br>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"> <li>• The password may not be the same as the username, regardless of case.</li> <li>• The password may not be the same as the username in reverse, regardless of case.</li> <li>• The password may not be the same as the username or reversed username with the following character substitutions:               <ul style="list-style-type: none"> <li>– "@" or "4" for "a"</li> <li>– "3" for "e"</li> <li>– "l", "!", or "1" for "i"</li> <li>– "0" for "o"</li> <li>– "\$" or "5" for "s"</li> <li>– "+" or "7" for "t"</li> </ul> </li> </ul> |
| Password Rules:<br>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.<br><br>You can enter any number from one (1) to 15. Default is three (3).                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 3** Submit and commit your changes.

## Changing Passwords

To change passwords for users configured on the system, use the Edit User page in the GUI (see [Editing Users, page 12-58](#) for more information).

To change the password for the default admin user account for the system, use the Edit User page in the GUI (see [Editing Users, page 12-58](#) for more information) or use the `password` or `passwd` command in the CLI. If you forget the password for the admin user account, contact your customer support provider to reset the password.

Users can change their own passwords by clicking the Options menu at the top of the GUI and selecting the Change Password option.

**Figure 12-21** *Change Password Page*

### Change Password

Enter the old password, and then enter the new password and reenter it for confirmation. Click **Submit** to log out. The login screen appears.

## 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, perform the following:

- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > Users**.



**Note** If the appliance cannot communicate with the external directory, the user can log in with a local user account on the appliance.

**Figure 12-22 Enabling External Authentication**



**Note** To set up the appliance to use an external directory for authentication, use the **userconfig** command and the **external** subcommand at the command line prompt.

## 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.

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 chapter on LDAP queries in the *Cisco IronPort AsyncOS for Email Advanced User Guide*.

To enable external authentication using LDAP:

- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > Users** page.
- Step 2** Click **Enable**.

The Edit External Authentication page appears.

**Figure 12-23 Enabling External Authentication Using LDAP**

**Edit External Authentication**

External Authentication Settings

☒ **Enable External Authentication**

Authentication Type: LDAP

LDAP External Authentication Query: Test.externalauth

Timeout to wait for valid response from server: seconds

| Group Name in Directory | Role  |
|-------------------------|-------|
|                         | Guest |

Cancel Submit

- Step 3** Select the Enable External Authentication check box.
- Step 4** Select LDAP for the authentication type.
- 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** Click **Submit** and then click **Commit** to 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 Management Appliance > 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 12-24 Enabling External Authentication Using RADIUS**  
Edit External Authentication

**External Authentication Settings**

☒ **Enable External Authentication**

Authentication Type: **RADIUS**

**RADIUS Server Information:**

| RADIUS Server Hostname | Port | Shared Secret | Timeout Value (in seconds) | Authentication protocol | Add Row |
|------------------------|------|---------------|----------------------------|-------------------------|---------|
|                        | 1812 |               | 5                          | PAP                     |         |

External Authentication Cache Timeout: 0 seconds

**Group Mapping:**

☒ Map externally authenticated users to multiple IronPort roles. (recommended)

| RADIUS CLASS Attribute | Role          | Add Row |
|------------------------|---------------|---------|
|                        | Administrator |         |

RADIUS CLASS attributes are case-sensitive.

☐ Map all externally authenticated users to the Administrator role.

Cancel Submit

- 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.
- 

## Configuring Access to the Security Management Appliance

AsyncOS provides administrators controls to manage users' access to the Security Management appliance, including a timeout for Web UI session and an access list that specifies the IP addresses from which users and your organization's proxy servers can access the appliance.



## Configuring IP-Based Network Access

You can control from which IP addresses users access the Security Management appliance by creating access lists for users who connect directly to the appliance and users who connect through a reverse proxy, if your organization uses reverse proxies for remote users.

### Direct Connections

You can specify the IP addresses, subnets, or CIDR addresses for machines that can connect to the Security Management appliance. Users can access the appliance from any machine with IP address from the access list. Users attempting to connect to the appliance from an address not included in the list are denied access.

### Connecting Through a Proxy

If your organization's network uses reverse proxy servers between remote users' machines and the Security Management appliance, AsyncOS allows you create an access list with the IP addresses of the proxies that can connect to the appliance.

Even when using a reverse proxy, AsyncOS still validates the IP address of the remote user's machine against a list of IP addresses allowed for user connections. To send the remote user's IP address to the Email Security appliance, the proxy needs to include the `x-forwarded-for` HTTP header in its connection request to the appliance.

The `x-forwarded-for` header is a non-RFC standard HTTP header with the following format:

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

The value for this header is a comma-separated list of IP addresses with the left-most address being the address of the remote user's machine, followed by the addresses of each successive proxy that forwarded the connection request. (The header name is configurable.) The Security Management appliance matches the remote user's IP address from the header and the connecting proxy's IP address against the allowed user and proxy IP addresses in the access list.

**Note**

---

AsyncOS supports only IPv4 addresses in the `x-forwarded-for` header.

---

## Creating the Access List

You can create the network access list either via the Network Access page in the GUI or the **adminaccessconfig > ipaccess** CLI command. Figure 12-25 shows the Network Access page with a list of user IP addresses that are allowed to connect directly to the Security Management appliance.

**Figure 12-25 Network Access Settings**  
Network Access

**Network Access**

Web UI Inactivity Timeout: 30 Minutes  
Enter a value between 5 - 1440 Minutes (24 hours).

User Access: Control system access by IP Address, IP Range or CIDR.  
Only Allow Specific Connections

10.0.0.33/32, 10.0.0.52/32, 10.0.0.130/32, 10.0.0.105/32, 10.0.0.155/32,  
10.0.0.23/32, 10.0.0.28/32, 10.0.0.209/32, 10.0.0.31/32, 10.0.0.60/32,  
10.0.0.51/32

(Valid entries are an IP address, IP range or CIDR range. Separate multiple entries with commas.  
Examples: 10.0.0.1, 10.0.0.1-24, 10.0.0.0/8)

IP Address of Proxy Server:

(Separate multiple entries with commas.)

Origin IP Header:  
x-forwarded-for

Cancel Submit

AsyncOS offers four different modes of control for the access list:

- **Allow All.** This mode allows all connections to the appliance. This is the default mode of operation.
- **Only Allow Specific Connections.** This mode allows a user to connection to the appliance if the user's IP address matches the IP addresses, IP ranges, or CIDR ranges included in the access list.
- **Only Allow Specific Connections Through Proxy.** This mode allows a user to connect to the appliance through a reverse proxy if the following conditions are met:
  - The connecting proxy's IP address is included in the access list's IP Address of Proxy Server field.

- The proxy includes the `x-forwarded-header` HTTP header in its connection request.
  - The value of `x-forwarded-header` is not empty.
  - The remote user's IP address is included in `x-forwarded-header` and it matches the IP addresses, IP ranges, or CIDR ranges defined for users in the access list.
- **Only Allow Specific Connections Directly or Through Proxy.** This mode allows users to connect through a reverse proxy or directly to the appliance if their IP address matches the IP addresses, IP ranges, or CIDR ranges included in the access list. The conditions for connecting through a proxy are the same as in the Only Allow Specific Connections Through Proxy mode.

Please be aware that you may lose access to the appliance after submitting and committing your changes if one of the following conditions is true:

- If you select **Only Allow Specific Connections** and do not include the IP address of your current machine in the list.
- If you select **Only Allow Specific Connections Through Proxy** and the IP address of the proxy currently connected to the appliance is not in the proxy list and the value of the Origin IP header is not in the list of allowed IP addresses.
- If you select **Only Allow Specific Connections Directly or Through Proxy** and
  - the value of the Origin IP header is not in the list of allowed IP addresses
  - OR
  - the value of the Origin IP header is not in the list of allowed IP Addresses and the IP address of the proxy connected to the appliance is not in the list of allowed proxies.

If you choose to continue without correcting the access list, AsyncOS will disconnect your machine or proxy from the appliance when you commit your changes.

To create an access list for the Security Management appliance:

- 
- Step 1** Use the **System Administration > Network Access** page.
  - Step 2** Click **Edit Settings**.
  - Step 3** Select the mode of control for the access list.

- Step 4** Enter the IP addresses from which users will be allowed to connect to the appliance.
- You can enter an IP address, IP address range or CIDR range. Use commas to separate multiple entries.
- Step 5** If connecting through a proxy is allowed, enter the following information:
- The IP addresses of the proxies allowed to connect to the appliance. Use commas to separate multiple entries.
  - The name of the origin IP header that the proxy sends to the appliance, which contains the IP addresses of the remote user's machine and the proxy servers that forwarded the request. By default, the name of the header is `x-forwarded-for`.
- Step 6** Submit and commit your changes.
- 

## Configuring the Web UI Session Timeout

You can specify how long a user can be logged into the Security Management appliance's Web UI before AsyncOS logs the user out due to inactivity. This Web UI session timeout applies to all users, including admin, and it is used for both HTTP and HTTPS sessions.

Once AsyncOS logs a user out, the appliance redirects the user's web browser to login page.



### Note

The Web UI Session Timeout does not apply to IronPort Spam Quarantine sessions, which have a 30 minute timeout that cannot be configured.

---

**Figure 12-26** Web UI Inactivity Timeout



To define the inactivity timeout for the Web UI session:

---

- Step 1** Use the **System Administration > Network Access** page.
- Step 2** Click **Edit Settings**.

- Step 3** Enter the number of minutes users can be inactive before being logged out. You can define a timeout period between 5 and 1440 minutes.
- Step 4** Submit and commit your changes.

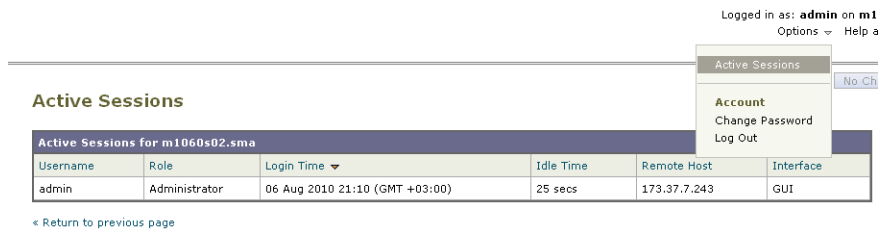
## Viewing Active Sessions

From the Security Management appliance, you can view all active sessions and logged in users on the appliance.

To view the active sessions, perform the following:

- Step 1** On the Security Management appliance page, choose **Options > Active Sessions**. The Active Sessions page appears.

**Figure 12-27 Active Sessions Page**



From the Active Sessions page you can view the User name, what role the user has, the time the user logged in, idle time, and whether the user is logging in from the command line or the GUI.

# Configuring the Return Address for Generated Messages

You can configure the envelope sender for mail generated by AsyncOS for the following types of cases:

- Bounce messages
- Reports

You can specify the display, user, and domain names of the return address. You can also choose to use the Virtual Gateway domain for the domain name.

Use the Return Addresses page available on the System Administration menu in the GUI, or use the **addressconfig** command in the CLI.

**Figure 12-28**      *Return Addresses Page*

## Return Addresses

| Return Addresses for System-Generated Email |                                                 |
|---------------------------------------------|-------------------------------------------------|
| Bounce Messages:                            | "Mail Delivery System" <MAILER-DAEMON@hostname> |
| Reports:                                    | "IronPort Reporting" <reporting@hostname>       |
| All Other Messages:                         | "Mail Delivery System" <MAILER-DAEMON@hostname> |
| <a href="#">Edit Settings...</a>            |                                                 |

To modify the return address for system-generated email messages in the GUI, click **Edit Settings** on the Return Addresses page. Make changes to the address or addresses you want to modify, click **Submit**, and commit your changes.

## Managing Alerts

Alerts are email notifications containing information about events occurring on the Cisco IronPort appliance. These events can be of varying levels of importance (or severity) from minor to major and pertain generally to a specific component or feature on your appliance. Alerts are generated by the Cisco IronPort appliance. You can specify, at a much more granular level, which alert messages are sent to which users and for which severity of event they are sent. Manage alerts on the Management Appliance > System Administration > Alerts page in the GUI (or via the **alertconfig** command in the CLI).

## Overview of Alerts

The following features control the behavior of email notifications:

- **Alerts:** Create alerts to receive email notifications. An alert consists of alert recipients (the email addresses for receiving alerts), and the alert notification (including the severity and alert type).
- **Alert Settings:** Specify global behavior for the alerting feature, including alert sender (FROM:) address, seconds to wait between sending duplicate alerts, and whether to enable AutoSupport (and optionally send weekly AutoSupport reports).

### Alerts: Alert Recipients, Alert Classifications, and Severities

Alerts are email messages or notifications containing information about specific functions, such as hardware problems, that are sent to an alert recipient. An alert recipient is an email address to which the alert notifications are sent. The information contained in the notification is determined by the alert classification and severity. You can specify which alert classifications, at which severity, are sent to a particular alert recipient. The alerting engine allows for granular control over the alerts that are sent to recipients. For example, you can configure the system to send only specified types of alerts to a recipient, such as when the severity level is Critical and the alert type is System. You can also configure general settings (see [Configuring Alert Settings, page 12-83](#)). See [Alert Listing, page 12-84](#) for a complete list of alerts.

#### Alert Classifications

AsyncOS sends the following alert classifications:

- System
- Hardware

#### Severities

Alerts can be sent for the following severities:

- Critical: issue that requires immediate attention
- Warning: problem or error requiring further monitoring and potentially immediate attention

- Info: information generated in the routine functioning of this device

## Alert Settings

Alert settings control the general behavior and configuration of alerts, including:

- The RFC 2822 Header From: when sending alerts (enter an address or use the default “alert@<hostname>”). You can also set this via the CLI, using the `alertconfig -> from` command.
- The initial number of seconds to wait before sending a duplicate alert.
- The maximum number of seconds to wait before sending a duplicate alert.
- The status of AutoSupport (enabled or disabled).
- The sending of AutoSupport’s weekly status reports to alert recipients set to receive system alerts at the Information level.

### Sending Duplicate Alerts

You can specify the initial number of seconds to wait before AsyncOS will send a duplicate alert. If you set this value to 0, duplicate alert summaries are not sent; instead, all duplicate alerts are sent without any delay (this can lead to a large amount of email over a short amount of time). The number of seconds to wait between sending duplicate alerts (alert interval) is increased after each alert is sent. The increase is the number of seconds to wait plus twice the last interval. So a 5-second wait would have alerts sent at 5 seconds, 15 seconds, 35 seconds, 75 seconds, 155 seconds, 315 seconds, and so on.

Eventually, the interval could become large. You can set a cap on the number of seconds to wait between intervals via the maximum number of seconds to wait before sending a duplicate alert field. For example, if you set the initial value to 5 seconds, and the maximum value to 60 seconds, alerts would be sent at 5 seconds, 15 seconds, 35 seconds, 60 seconds, 120 seconds, and so on.

## Alert Delivery

Because alert messages can be used to inform you of problems within your Cisco IronPort appliance, they are not sent using AsyncOS’s normal mail delivery system. Instead, alert messages pass through a separate and parallel email system designed to operate even in the face of significant system failure in AsyncOS.



The alert mail system does not share the same configuration as AsyncOS, which means that alert messages may behave slightly differently from other mail delivery:

- Alert messages are delivered using standard DNS MX and A record lookups.
  - They do not use SMTP routes in AsyncOS versions older than 5.X.
  - They do cache the DNS entries for 30 minutes and the cache is refreshed every 30 minutes, so in case of DNS failure the alerts still go out.
- Alert messages do not pass through the work queue, so they are not scanned for viruses or spam. They are also not subjected to message filters or content filters.
- Alert messages do not pass through the delivery queue, so they will not be affected by bounce profiles or destination control limits.

## SMTP Routes and Alerts

Alerts sent from the appliance to addresses specified in the Alert Recipients section follow SMTP routes defined for those destinations.

## Cisco IronPort AutoSupport

To allow Cisco IronPort to better support and design future system changes, the Cisco IronPort appliance can be configured to send Cisco IronPort Systems a copy of all alert messages generated by the system. This feature, called ‘AutoSupport’, is a useful way to allow Cisco IronPort Customer Support to be proactive in supporting your needs. AutoSupport also sends weekly reports noting the uptime of the system, the output of the **status** command, and the AsyncOS version used.

By default, alert recipients set to receive Information severity level alerts for System alert types receive a copy of every message sent to Cisco IronPort. This can be disabled if you do not want to send the weekly alert messages internally. To enable or disable this feature, see [Configuring Alert Settings, page 12-83](#).

## Alert Messages

Alert messages are standard email messages. Although you can configure the Header From: address, the rest of the message is generated automatically.

## Alert From Address

You can configure the Header From: address by clicking the **Edit Settings** button in the GUI or by using the CLI (see the *Cisco IronPort AsyncOS CLI Reference Guide*).

## Alert Subject

An alert message's subject has the following format:

```
Subject: [severity]-[hostname]: ([class]) short message
```

## Example Alert Message

```
Date: 23 Mar 2007 21:10:19 +0000
```

```
To: joe@example.com
```

```
From: Cisco IronPort M650 Alert [alert@example.com]
```

```
Subject: Critical-example.com: (AntiVirus) update via  
http://newproxy.example.com failed
```

The Critical message is:

```
update via http://newproxy.example.com failed
```

```
Version: 6.0.0-419
```

```
Serial Number: XXXXXXXXXXXX-XXXXXXX
```

```
Timestamp: Tue May 10 09:39:24 2007
```

For more information about this error, please see

<http://support.ironport.com>

If you need further information, contact your support provider.

## Managing Alert Recipients

Log in to the GUI and select System Administration > Alerts. (For information about how to access the GUI, see [Accessing the Graphical User Interface, page 2-8.](#))

**Figure 12-29 Alerts Page**

### Alerts

Success — The recipient has been saved.

| Alert Recipients                 |        |          |        |
|----------------------------------|--------|----------|--------|
| <a href="#">Add Recipient...</a> |        |          |        |
| Recipient Address                | System | Hardware | Delete |
| admin@ironport.com               | All    | All      |        |

| Alert Settings                                                      |                         |
|---------------------------------------------------------------------|-------------------------|
| From Address to Use When Sending Alerts:                            | Automatically Generated |
| Initial Number of Seconds to Wait Before Sending a Duplicate Alert: | 300                     |
| Maximum Number of Seconds to Wait Before Sending a Duplicate Alert: | 3600                    |
| IronPort AutoSupport:                                               | Disabled                |
| <a href="#">Edit Settings...</a>                                    |                         |



#### Note

If you enabled AutoSupport during system setup, the email address that you specified will receive alerts for all severities and classes by default. You can change the configuration at any time.

The Alerts page lists the existing alert recipients and alert settings.

From the Alerts page, you can:

- Add, configure, or delete alert recipients.

- Modify the alert settings.

## Adding New Alert Recipients

To add a new alert recipient:

- Step 1

Click **Add Recipient** on the Alerts page. The Add Alert Recipients page appears.

**Figure 12-30**     *Adding an Alert Recipient*

### Add Alert Recipient

| Alert Recipient    |                                                                             |                          |                          |                          |
|--------------------|-----------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|
| Recipient Address: | <div></div> <div><i>Separate multiple email addresses with commas</i></div> |                          |                          |                          |
|                    | Alert Severities to Receive                                                 |                          |                          |                          |
|                    | All                                                                         | Critical ?               | Warning ?                | Info ?                   |
| Alert Type         | <input type="checkbox"/>                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| System             | <input type="checkbox"/>                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Hardware           | <input type="checkbox"/>                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Cancel

Submit

- Step 2

Enter the recipient’s email address. You can enter multiple addresses, separated by commas.
- Step 3

Select the alert severities that the alert recipient will receive.
- Step 4

Click **Submit** to add the alert recipient.
- Step 5

Commit your changes.

## Configuring Existing Alert Recipients

To edit an existing alert recipient:

- Step 1

Click the alert recipient in the Alert Recipients listing. The Configure Alert Recipient page appears.
- Step 2

Make changes to the alert recipient.

- Step 3** Submit and commit your changes.
- 

## Deleting Alert Recipients

To delete an alert recipient:

- 
- Step 1** Click the trash can icon corresponding to the alert recipient in the Alert Recipient listing.
- Step 2** Confirm the deletion by clicking **Delete** in the warning dialog that appears.
- Step 3** Commit your changes.
- 

## Configuring Alert Settings

Alert settings are global settings, meaning that they affect how all of the alerts behave.

## Editing Alert Settings

To edit alert settings:

- 
- Step 1** Click **Edit Settings** on the Alerts page. The Edit Alert Settings page appears.

Figure 12-31 Editing Alert Settings

Edit Alert Settings

Alert Settings

From Address to Use When Sending Alerts:

Automatically generated  
(example: IronPort C60 Alert <alert@host.example.com>)

Wait Before Sending a Duplicate Alert:

☒ Enable

Initial Number of Seconds to Wait Before Sending a Duplicate Alert  
 Maximum Number of Seconds to Wait Before Sending a Duplicate Alert

IronPort AutoSupport:

☒ Enable

☒ Send copy of weekly AutoSupport reports to System Information Alert recipients.

Cancel

Submit

- Step 2

Enter a Header From: address to use when sending alerts, or select “Automatically generated” (“alert@<hostname>”).
- Step 3

Select the check box if you want to specify the number of seconds to wait between sending duplicate alerts. For more information, see [Sending Duplicate Alerts, page 12-78](#).

  - Specify the initial number of seconds to wait before sending a duplicate alert.
  - Specify the maximum number of seconds to wait before sending a duplicate alert.
- Step 4

Optionally, enable AutoSupport by selecting the Cisco IronPort AutoSupport option. For more information about AutoSupport, see [Cisco IronPort AutoSupport, page 12-79](#).

  - If AutoSupport is enabled, the weekly AutoSupport report is sent to alert recipients set to receive system alerts at the Information level. You can disable this via the check box.
- Step 5

Submit and commit your changes.

# Alert Listing

The following tables list alerts by classification, including the alert name, description, and severity.

## Hardware Alerts

Table 12-4 contains a list of the various hardware alerts that AsyncOS can generate, including a description of the alert and the alert severity.

**Table 12-4**      *Listing of Hardware Alerts*

| Alert Name                                   | Description                                                                        | Severity    |
|----------------------------------------------|------------------------------------------------------------------------------------|-------------|
| <b>INTERFACE.ERRORS</b>                      | Sent when interface errors are detected.                                           | Warning     |
| <b>MAIL.MEASUREMENTS_FILESYSTEM</b>          | Sent when a disk partition is nearing capacity (75%).                              | Warning     |
| <b>MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL</b> | Sent when a disk partition reaches 90% capacity (and at 95%, 96%, 97%, and so on). | Critical    |
| <b>SYSTEM.RAID_EVENT_ALERT</b>               | Sent when a critical RAID-event occurs.                                            | Warning     |
| <b>SYSTEM.RAID_EVENT_ALERT_INFO</b>          | Sent when a RAID-event occurs.                                                     | Information |

## System Alerts

Table 12-5 contains a list of the various system alerts that AsyncOS can generate, including a description of the alert and the alert severity.

**Table 12-5**      *Listing of System Alerts*

| Alert Name                             | Description                                                        | Severity |
|----------------------------------------|--------------------------------------------------------------------|----------|
| <b>COMMON.APP_FAILURE</b>              | Sent when there is an unknown application failure.                 | Critical |
| <b>COMMON.KEY_EXPIRED_ALERT</b>        | Sent when a feature key has expired.                               | Warning  |
| <b>COMMON.KEY_EXPIRING_ALERT</b>       | Sent when a feature key is about to expire.                        | Warning  |
| <b>COMMON.KEY_FINAL_EXPIRING_ALERT</b> | Sent as a final notice that a feature key is about to expire.      | Warning  |
| <b>DNS.BOOTSTRAP_FAIL</b>              | Sent when the appliance is unable to contact the root DNS servers. | Warning  |

**Table 12-5 Listing of System Alerts (continued)**

| <b>Alert Name</b>                                    | <b>Description</b>                                                                                                 | <b>Severity</b> |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>INTERFACE.FAILOVER.FAILURE_BACKUP_DETECTED</b>    | Sent when a backup NIC pairing interface fails.                                                                    | Warning         |
| <b>INTERFACE.FAILOVER.FAILURE_BACKUP_RECOVERED</b>   | Sent when a NIC pair failover is recovered.                                                                        | Information     |
| <b>INTERFACE.FAILOVER.FAILURE_DETECTED</b>           | Sent when a NIC pairing failover is detected due to an interface failure.                                          | Critical        |
| <b>INTERFACE.FAILOVER.FAILURE_DETECTED_NO_BACKUP</b> | Sent when a NIC pairing failover is detected due to an interface failure, but a backup interface is not available. | Critical        |
| <b>INTERFACE.FAILOVER.FAILURE_RECOVERED</b>          | Sent when a NIC pair failover is recovered.                                                                        | Information     |
| <b>INTERFACE.FAILOVER.MANUAL</b>                     | Sent when a manual failover to another NIC pair is detected.                                                       | Information     |
| <b>COMMON.INVALID_FILTER</b>                         | Sent when an invalid filter is encountered.                                                                        | Warning         |
| <b>LDAP.GROUP_QUERY_FAILED_ALERT</b>                 | Sent when an LDAP group query fails.                                                                               | Critical        |
| <b>LDAP.HARD_ERROR</b>                               | Sent when an LDAP query fails completely (after trying all servers).                                               | Critical        |
| <b>LOG.ERROR.*</b>                                   | Various logging errors.                                                                                            | Critical        |
| <b>MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED</b>          | Sent when an LDAP group query fails during per-recipient scanning.                                                 | Critical        |
| <b>MAIL.QUEUE.ERROR.*</b>                            | Various mail queue hard errors.                                                                                    | Critical        |
| <b>MAIL.RES_CON_START_ALERT.MEMORY</b>               | Sent when RAM utilization has exceeded the system resource conservation threshold.                                 | Critical        |
| <b>MAIL.RES_CON_START_ALERT.QUEUE_SLOW</b>           | Sent when the mail queue is overloaded and system resource conservation is enabled.                                | Critical        |



**Table 12-5 Listing of System Alerts (continued)**

| <b>Alert Name</b>                                        | <b>Description</b>                                                                                                                                                | <b>Severity</b> |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>MAIL.RES_CON_START_ALERT.QUEUE</b>                    | Sent when queue utilization has exceeded the system resource conservation threshold.                                                                              | Critical        |
| <b>MAIL.RES_CON_START_ALERT.WORKQ</b>                    | Sent when listeners are suspended because the work queue size is too big.                                                                                         | Critical        |
| <b>MAIL.RES_CON_START_ALERT</b>                          | Sent when the appliance enters “resource conservation” mode.                                                                                                      | Critical        |
| <b>MAIL.RES_CON_STOP_ALERT</b>                           | Sent when the appliance leaves “resource conservation” mode.                                                                                                      | Critical        |
| <b>MAIL.WORK_QUEUE_PAUSED_NATURAL</b>                    | Sent when the work queue is paused.                                                                                                                               | Critical        |
| <b>MAIL.WORK_QUEUE_UNPAUSED_NATURAL</b>                  | Sent when the work queue is resumed.                                                                                                                              | Critical        |
| <b>NTP.NOT_ROOT</b>                                      | Sent when the Cisco IronPort appliance is unable to adjust time because NTP is not running as root.                                                               | Warning         |
| <b>PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS</b> | Sent when errors are found in the domain specification file.                                                                                                      | Critical        |
| <b>PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY</b>         | Sent when the domain specification file is empty.                                                                                                                 | Critical        |
| <b>PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING</b>       | Sent when the domain specification file is not found.                                                                                                             | Critical        |
| <b>REPORTD.DATABASE_OPEN_FAILED_ALERT</b>                | Sent if the reporting engine is unable to open the database.                                                                                                      | Critical        |
| <b>REPORTD.AGGREGATION_DISABLED_ALERT</b>                | Sent if the system runs out of disk space. When the disk usage for a log entry exceeds the log usage threshold, reportd disables aggregation and sends the alert. | Warning         |
| <b>REPORTING.CLIENT.UPDATE_FAILED_ALERT</b>              | Sent if the reporting engine was unable to save reporting data.                                                                                                   | Warning         |
| <b>REPORTING.CLIENT.JOURNAL.FULL</b>                     | Sent if the reporting engine is unable to store new data.                                                                                                         | Critical        |

**Table 12-5 Listing of System Alerts (continued)**

| <b>Alert Name</b>                                         | <b>Description</b>                                                                                | <b>Severity</b> |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------|
| <b>REPORTING.CLIENT.JOURNAL.FREE</b>                      | Sent when the reporting engine is again able to store new data.                                   | Information     |
| <b>PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE_ALERT</b>   | Sent when the reporting engine is unable to build a report.                                       | Critical        |
| <b>PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE_ALERT</b>   | Sent when a report could not be emailed.                                                          | Critical        |
| <b>PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE_ALERT</b> | Sent when a report could not be archived.                                                         | Critical        |
| <b>SENDERBASE.ERROR</b>                                   | Sent when an error occurred while processing a response from SenderBase.                          | Information     |
| <b>SMAD.ICCM.ALERT_PUSH_FAILED</b>                        | Sent if a configuration push failed for one or more hosts.                                        | Warning         |
| <b>SMAD.TRANSFER.TRANSFERS_STALLED</b>                    | Sent if SMA logs are unable to fetch tracking data for two hours or reporting data for six hours. | Warning         |
| <b>SMTPAUTH.FWD_SERVER_FAILED_ALERT</b>                   | Sent when the SMTP Authentication forwarding server is unreachable.                               | Warning         |
| <b>SMTPAUTH.LDAP_QUERY_FAILED</b>                         | Sent when an LDAP query fails.                                                                    | Warning         |
| <b>SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT</b>              | Sent when there was a problem shutting down the system on reboot.                                 | Warning         |
| <b>SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN</b>            | Sent when there was a problem shutting down the system.                                           | Warning         |
| <b>SYSTEM.RCPTVALIDATION.UPDATE_FAILED</b>                | Sent when a recipient validation update failed.                                                   | Critical        |

**Table 12-5**      *Listing of System Alerts (continued)*

| Alert Name                            | Description                                                                 | Severity    |
|---------------------------------------|-----------------------------------------------------------------------------|-------------|
| <b>SYSTEM.SERVICE_TUNNEL.DISABLED</b> | Sent when a tunnel created for Cisco IronPort Support Services is disabled. | Information |
| <b>SYSTEM.SERVICE_TUNNEL.ENABLED</b>  | Sent when a tunnel created for Cisco IronPort Support Services is enabled.  | Information |

## Changing Network Settings

This section describes the features used to configure the network operation of the Cisco IronPort appliance. These features give you direct access to the hostname, DNS, and routing settings that you configured using the System Setup Wizard in [Understanding the System Setup Wizard, page 2-9](#).

The following features are described:

- `sethostname`
- DNS configuration (in the GUI and by using the `dnsconfig` command in the CLI)
- Routing configuration (in the GUI and by using the `routeconfig` and `setgateway` commands in the CLI)
- `dnsflush`
- Password

## Changing the System Hostname

The hostname is used to identify the system at the CLI prompt. You must enter a fully qualified hostname. The `sethostname` command sets the name of the Cisco IronPort appliance. The new hostname does not take effect until you issue the `commit` command.

## The sethostname Command

```
oldname.example.com> sethostname
```

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

```
oldname.example.com>
```

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

```
oldname.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Changed System Hostname
```

```
Changes committed: Mon Jan 04 12:00:01 2010
```

The new hostname appears in the prompt as follows: `mail3.example.com>`

## Configuring Domain Name System Settings

You can configure the Domain Name System (DNS) settings for your Cisco IronPort appliance through the Management Appliance > Network > DNS page in the GUI, or via the `dnsconfig` command.

You can configure the following settings:

- Whether to use the Internet's DNS servers or your own, and which server(s) to use
- Which interface to use for DNS traffic

- The number of seconds to wait before timing out a reverse DNS lookup
- Clearing the DNS cache

## Specifying DNS Servers

AsyncOS can use the Internet root DNS servers, your own DNS servers, or the Internet root DNS servers and authoritative DNS servers that you specify. When using the Internet root servers, you may specify alternate servers to use for specific domains. Because an alternate DNS server applies to a single domain, it must be authoritative (provide definitive DNS records) for that domain.

AsyncOS supports “splitting” DNS servers when not using the Internet’s DNS servers. If you are using your own internal server, you can also specify exception domains and associated DNS servers.

When setting up “split DNS,” you should set up the in-addr.arpa (PTR) entries as well. For example, if you want to redirect “.eng” queries to the nameserver 1.2.3.4 and all the .eng entries are in the 172.16 network, then you should specify “eng.16.172.in-addr.arpa” as the domains in the split DNS configuration.

## Multiple Entries and Priority

For each DNS server that you enter, you can specify a numeric priority. AsyncOS attempts to use the DNS server with the priority closest to 0. If that DNS server is not responding, AsyncOS attempts to use the server at the next priority. If you specify multiple entries for DNS servers with the same priority, the system randomizes the list of DNS servers at that priority every time it performs a query. The system then waits a short amount of time for the first query to expire or “time out” and then a slightly longer amount of time for the second, and so on. The amount of time depends on the exact total number of DNS servers and priorities that have been configured. The timeout length is the same for all IP addresses at any particular priority. The first priority gets the shortest timeout; each subsequent priority gets a longer timeout. Further, the timeout period is roughly 60 seconds. If you have one priority, the timeout for each server at that priority is 60 seconds. If you have two priorities, the timeout for each server at the first priority is 15 seconds, and each server at the second priority is 45 seconds. For three priorities, the timeouts are 5, 10, 45.

For example, suppose you configure four DNS servers, with two of them at priority 0, one at priority 1, and one at priority 2:

**Table 12-6**      *Example of DNS Servers, Priorities, and Timeout Intervals*

| Priority | Server(s)        | Timeout (Seconds) |
|----------|------------------|-------------------|
| 0        | 1.2.3.4, 1.2.3.5 | 5, 5              |
| 1        | 1.2.3.6          | 10                |
| 2        | 1.2.3.7          | 45                |

AsyncOS randomly chooses between the two servers at priority 0. If one of the priority 0 servers is down, the other is used. If both of the priority 0 servers are down, the priority 1 server (1.2.3.6) is used, and then, finally, the priority 2 (1.2.3.7) server.

The timeout period is the same for both priority 0 servers, longer for the priority 1 server, and longer still for the priority 2 server.

## Using the Internet Root Servers

The AsyncOS DNS resolver is designed to accommodate the large number of simultaneous DNS connections required for high-performance email delivery.



**Note**

If you choose to set the default DNS server to something other than the Internet root servers, that server must be able to recursively resolve queries for domains for which it is not an authoritative server.

## Reverse DNS Lookup Timeout

The Cisco IronPort appliance attempts to perform a “double DNS lookup” on all remote hosts connecting to a listener for the purposes of sending or receiving email. That is, the system acquires and verifies the validity of the remote host's IP address by performing a double DNS lookup. This consists of a reverse DNS (PTR) lookup on the IP address of the connecting host, followed by a forward DNS (A) lookup on the results of the PTR lookup. The system then checks that the results of the A lookup match the results of the PTR lookup. If the results do not match, or if an A record does not exist, the system uses only the IP address to

match entries in the Host Access Table (HAT). This particular timeout period applies only to this lookup and is not related to the general DNS timeout discussed in [Multiple Entries and Priority, page 12-91](#).

The default value is 20 seconds. You can disable the reverse DNS lookup timeout globally across all listeners by entering '0' as the number of seconds. If the value is set to 0 seconds, the reverse DNS lookup is not attempted, and instead the standard timeout response is returned immediately.

## DNS Alert

Occasionally, an alert may be generated with the message “Failed to bootstrap the DNS cache” when an appliance is rebooted. The message means that the system was unable to contact its primary DNS servers, which can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not pointing to a valid server.

## Clearing the DNS Cache

The **Clear Cache** button from the GUI, or the `dnsflush` command (for more information about the `dnsflush` command, see the *Cisco IronPort AsyncOS CLI Reference Guide*), clears all information in the DNS cache. You may choose to use this feature when changes have been made to your local DNS system. The command takes place immediately and may cause a temporary performance degradation while the cache is repopulated.

## Configuring DNS Settings via the Graphical User Interface

Log in to the GUI and select Management Appliance > Network > DNS.

Figure 12-32 DNS Page

DNS

DNS Server Settings

DNS Servers:

Use these DNS Servers:

| Priority | IP Address  |
|----------|-------------|
| 0        | 192.168.0.3 |

Interface for DNS traffic: Auto

Wait Before Timing out Reverse DNS Lookups: 20

Clear DNS Cache

Edit Settings...

To edit DNS settings in the GUI:

- Step 1
- On the **Management Appliance > Network > DNS** page, click the **Edit Settings** button.

The Edit DNS page appears.

Figure 12-33 Edit DNS Page

Edit DNS

DNS Server Settings

DNS Servers:

☐ Use these DNS Servers

| Priority ? | Server IP | Add Row |
|------------|-----------|---------|
|            |           |         |

Alternate DNS servers Overrides (Optional):

| Domain(s)                       | DNS Server IP Address | Add Row |
|---------------------------------|-----------------------|---------|
|                                 |                       |         |
| i.e., example.com, example2.com | i.e., 10.0.0.3        |         |

☒ Use the Internet's Root DNS Servers

Alternate DNS servers Overrides (Optional):

| Domain            | DNS Server FQDN       | DNS Server IP Address | Add Row |
|-------------------|-----------------------|-----------------------|---------|
|                   |                       |                       |         |
| i.e., example.com | i.e., dns.example.com | i.e., 10.0.0.3        |         |

Interface for DNS Traffic: Auto

Wait Before Timing out Reverse DNS Lookups: 20

Cancel

Submit



- Step 2** Select whether to use the Internet's root DNS servers or your own internal DNS server(s), and specify authoritative DNS servers.
  - Step 3** If you want to use your own DNS server(s) or specify authoritative DNS servers, enter the server ID and click **Add Row**. Repeat this for each server. When entering your own DNS servers, specify a priority as well. For more information, see [Specifying DNS Servers, page 12-91](#).
  - Step 4** Choose an interface for DNS traffic.
  - Step 5** Enter the number of seconds to wait before canceling a reverse DNS lookup.
  - Step 6** Optionally, clear the DNS cache by clicking **Clear Cache**.
  - Step 7** Submit and commit your changes.
- 

## Configuring TCP/IP Traffic Routes

Some network environments require the use of traffic routes other than the standard default gateway. You can manage static routes in the GUI through the Management Appliance > Network > Routing page, or in the CLI by using the `routeconfig` command.

## Managing Static Routes in the GUI

You can create, edit, or delete static routes by using the Management Appliance > Network > Routing page. You can also modify the default gateway from this page.

### Adding Static Routes

To create a new static route:

- 
- Step 1** On the Management Appliance > Network > Routing page, click **Add Route** in the route listing. The Add Static Route page appears.

**Figure 12-34 Adding a Static Route**

**Add Static Route**

| Static Route Settings   |                      |
|-------------------------|----------------------|
| Route Name:             | <input type="text"/> |
| Destination IP Address: | <input type="text"/> |
| Gateway IP Address:     | <input type="text"/> |

CancelSubmit

- Step 2

Enter a name for the route.
- Step 3

Enter the destination IP address.
- Step 4

Enter the gateway IP address.
- Step 5

Submit and commit your changes.

Deleting Static Routes

To delete a static route:

- Step 1

Click the trash can icon corresponding to the static route name in the Static Routes listing.
- Step 2

Confirm the deletion by clicking **Delete** in the warning dialog that appears.
- Step 3

Commit your changes.

Editing Static Routes

To edit a static route:

- Step 1

Click the name of the route in the Static Route listing. The Edit Static Route page appears.
- Step 2

Make changes to the route.
- Step 3

Submit and commit your changes.

## Modifying the Default Gateway (GUI)

To modify the default gateway:

- Step 1** Click Default Route in the route listing on the Routing page. The Edit Static Route page appears.

**Figure 12-35** *Editing the Default Gateway*

### Edit Static Route

| Gateway Settings        |                                         |
|-------------------------|-----------------------------------------|
| Route Name:             | Default Router                          |
| Destination IP Address: | All Destinations                        |
| Gateway IP Address:     | <input type="text" value="172.19.0.1"/> |

- Step 2** Change the gateway IP address.
- Step 3** Submit and commit your changes.

## Configuring the Default Gateway

You can configure the default gateway via the GUI through the Management Appliance > Network > Routing page (see [Modifying the Default Gateway \(GUI\)](#), [page 12-97](#)) or via the `setgateway` command in the CLI.

## Changing the Admin User's Password

The password for the admin user can be changed via the GUI or the CLI.

To change the password via the GUI, use the Management Appliance > System Administration > Users page. For more information, see [Editing Users](#), [page 12-58](#).

To change the password for the `admin` user in the CLI, use the `password` command. Passwords must be six characters or longer. The `password` command requires you to enter the old password for security.



**Note**

Changes to the password take effect immediately and do not require you to carry out the **commit** command.

# Configuring the System Time

You can set the system time on the Cisco IronPort appliance and specify the time zone. Use the Management Appliance > System Administration > Time Zone page and the Management Appliance > System Administration > Time Settings page in the GUI. Alternatively, use the `ntpconfig`, `settime`, and `settz` commands in the CLI.

## Time Zone Page

The Time Zone page (available on the System Administration menu in the GUI) displays the time zone for the Cisco IronPort appliance. You can select a specific time zone or GMT offset.

## Selecting a Time Zone

To set the time zone for the Cisco IronPort appliance:

- Step 1** Click **Edit Settings** on the **Management Appliance > System Administration > Time Zone** page. The Edit Time Zone page appears.

**Figure 12-36** *Edit Time Zone Page*

**Edit Time Zone**

| Time Zone Setting |                                                                    |
|-------------------|--------------------------------------------------------------------|
| Time Zone:        | Region: <input type="text" value="America"/>                       |
|                   | Country: <input type="text" value="United States"/>                |
|                   | Time Zone: <input type="text" value="Pacific Time (Los_Angeles)"/> |

- Step 2** Select a region, country, and time zone.

**Step 3** Submit and commit your changes.

---

## Selecting a GMT Offset

To set the GMT offset for the Cisco IronPort appliance:

- Step 1** Click **Edit Settings** on the Management Appliance > System Administration > Time Zone page. The Edit Time Zone page appears.
- Step 2** Select GMT Offset from the list of regions. The Time Zone Setting page is updated to include GMT offsets in the Time Zone field.

**Figure 12-37** *Setting a GMT Offset*

### Edit Time Zone

| Time Zone Setting |            |                   |
|-------------------|------------|-------------------|
| Time Zone:        | Region:    | GMT Offset ▾      |
|                   | Country:   | GMT ▾             |
|                   | Time Zone: | GMT (GMT) ▾       |
| <div>Cancel</div> |            | <div>Submit</div> |

- Step 3** Select an offset in the Time Zone field. The offset refers to the number of hours that you add or subtract to or from Greenwich Mean Time (GMT) — the local time at the prime meridian. Hours preceded by a minus sign (“-”) are west of the prime meridian. A plus sign (“+”) indicates locations east of the prime meridian.
- Step 4** Submit and commit your changes.
- 



### Note

When gathering data for reports, the Security Management appliance applies the time stamp from the information that was set when you configured the time settings on the Security Management appliance. For information on how the Security Management appliance gathers information, see [“How the Security Appliance Gathers Data for Reports”](#) section on page 3-16.

---

## Editing Time Settings (GUI)

To edit the time settings for your Cisco IronPort appliance, click the **Edit Settings** button on the **Management Appliance > System Administration > Time Settings** page. The Edit Time Settings page appears.

**Figure 12-38** Edit Time Settings Page

### Edit Time Settings

**Time Settings**

Time Keeping Method: ☐ Use Network Time Protocol

NTP Server Add Row

|                   |  |
|-------------------|--|
| time.ironport.com |  |
|-------------------|--|

Interface for NTP Server Queries: Auto select

☒ Set Time Manually

Local Time:

MM/DD/YYYY HH:MM:SS

Note: manual time set will take place immediately when the Submit button is clicked — it is not necessary to “commit” these changes.

Cancel Submit

## Editing the Network Time Protocol (NTP) Configuration (Time Keeping Method)

To use an NTP server to synchronize the system clock with other computers and edit the NTP server settings:

- Step 1** Click **Edit Settings** on the Management Appliance > System Administration > Time Settings page. The Edit Time Settings page appears.
- Step 2** In the Time Keeping Method section, select Use Network Time Protocol.
- Step 3** Enter an NTP server address and click **Add Row**. You can add multiple NTP servers.
- Step 4** To delete an NTP server from the list, click the trash can icon for that server.
- Step 5** Select an interface for NTP queries. This is the IP address from which NTP queries should originate.
- Step 6** Submit and commit your changes.

## Setting System Time Without Using an NTP Server

To set the system time manually, without using an NTP server:

- 
- Step 1** Click **Edit Settings** on the Management Appliance > System Administration > Time Settings page. The Edit Time Settings page appears.
  - Step 2** In the Time Keeping Method section, select Set Time Manually.
  - Step 3** Enter the date in MM/DD/YYYY format, or click the calendar icon to select the date.
  - Step 4** Enter the local time in HH:MM:SS format.
  - Step 5** Submit and commit your changes.
- 

## Updating Time Zone Files

Each time zone file on the Security Management appliance contains rules that specify the relative time of a specific time zone. You can update the time zone files on the Security Management appliance any time between AsyncOS upgrades. Whenever there is a change in the time zone rules for any country, you may need to update these files on the appliance.

You can update the time zone files in the GUI, or CLI using the `tzupdate` command.

To update the time zone files in the GUI:

- 
- Step 1** Navigate to the Management Appliance > System Administration > Time Settings page.

### Time Settings

| Time Setting         |  |                                                     |  |
|----------------------|--|-----------------------------------------------------|--|
| Time Keeping Method: |  | Set Manually (current time: 3/31/2011, 11:48:40 PM) |  |
|                      |  | <a href="#">Edit Settings...</a>                    |  |

| Time Zone File Updates  |               |                 |                            |
|-------------------------|---------------|-----------------|----------------------------|
| Type                    | Last Update   | Current Version | New Update                 |
| Time zone rules         | Never updated | 2010.02.0       | Not Available              |
| No updates in progress. |               |                 | <a href="#">Update Now</a> |

- Step 2** If there is an available time zone file update, click **Update Now**.
- 

## Defining Time Ranges for Time-Based Policies

You can define time ranges such as “business hours” or “weekend shift” in order to restrict web-based activities to certain days and times. For example, you can block access to high-bandwidth or distracting sites during business hours.

For details, see “Working with Time Based Policies” in the “*Cisco IronPort AsyncOS for Web Security User Guide*.”

To add or edit a time range, perform the following:

- 
- Step 1** On the Security Management appliance, choose **Web > Configuration Master > Defined Time Ranges**.
- The Time Ranges page appears.
- Step 2** Click Add Time Range.
- The Add Time Range page appears.
- Step 3** In the Time Range Name text field, type the name of the time range.
- Step 4** In the Time Zone area choose the time zone you prefer by clicking on the radio button corresponding to your choice. Choices are:
- Use Time Zone Setting from Appliance
  - Specify Time Zone for this Time Range
- Select Region, Country and Time Zone from the corresponding drop-down menus.
- Step 5** In the Time Values area, select the days of the week for the defined time zone and the time of day.
- Step 6** Click on Add Row.
- Step 7** Click Submit.
-



# Managing the Configuration File

Most configuration settings for the Cisco IronPort appliance can be managed in a single configuration file. The file is maintained in Extensible Markup Language (XML) 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 an entire configuration file through FTP, or you can paste portions of a configuration file directly into the CLI.
- Because the file is in XML format, an associated document type definition (DTD) 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



### Warning

**If you want to import a configuration file from one Security Management appliance into another Security Management appliance:**

**Everything in the original configuration, including the IP Address, is included in the configuration file. Either edit the configuration file to change the IP address, or be sure the original Security Management appliance is offline.**

**Also, be aware that the SSH authentication connection will terminate. When this happens, you will need to re-establish the connection for all connected Web Security appliances and Email Security appliances.**

- 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. However, you cannot load configuration files from Email Security appliances onto a Security Management appliance.
- You can divide an existing configuration file downloaded from one appliance 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 in the GUI

To manage configuration files on your appliance, choose **Management Appliance > System Administration > Configuration File**.

The Configuration File page contains the following sections:

- **Current Configuration:** used to save and export the current configuration file
- **Load Configuration:** used to load a complete or partial configuration file
- **End-User Safelist/Blocklist Database (Cisco IronPort Spam Quarantine):** used to manage the safelist/blocklist database
- **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 Management Appliance > 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 12-39**      **Current Configuration File**

Mask the user's passwords by selecting the check box. Masking a password causes the original, encrypted password to be replaced with "\*\*\*\*\*" in the exported or saved file.



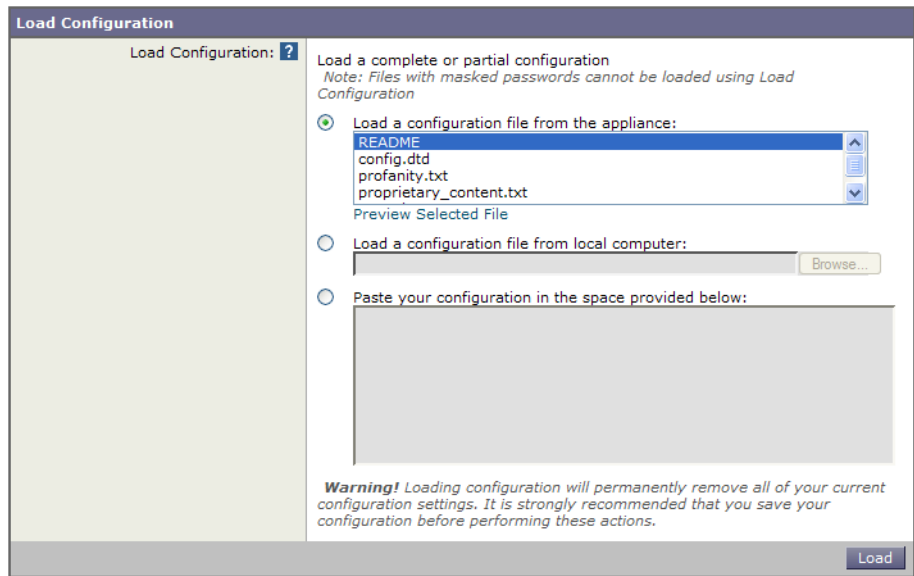
### Note

Configuration files with masked passwords cannot be loaded back into AsyncOS.

## Loading a Configuration File

Use the Load Configuration section of the Management Appliance > System Administration > Configuration File page to load new configuration information into the Cisco IronPort appliance. You can load information using one of three methods:

- Step 1** Placing information in the `configuration` directory and uploading it
  - Step 2** Uploading the configuration file directly from your local machine
  - Step 3** Pasting configuration information directly into the GUI
- Configuration files with masked passwords cannot be loaded.

**Figure 12-40 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 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* subsection 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 the following code causes validation errors:

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

<!DOCTYPE config SYSTEM "config.dtd">

<config>

    <autosupport_enabled>0</autosu

</config>
```

However, uploading or pasting the following code does not cause validation errors:

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

<!DOCTYPE config SYSTEM "config.dtd">

<config>

    <autosupport_enabled>0</autosupport_enabled>

</config>
```

“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 the following code (including the declarations and `<config></config>` tags) is allowed:

```
<hostname>mail4.example.com</hostname>
```

However, a system can have multiple listeners defined, each with different Recipient Access Tables defined, so uploading only the following code is considered ambiguous:

```
<rat>

  <rat_entry>

    <rat_address>ALL</rat_address>

    <access>RELAY</access>

  </rat_entry>

</rat>
```

Because it is ambiguous, it 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 Versus 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 the following code removes all listeners from the system:

```
<listeners></listeners>
```



#### Warning

**When uploading or pasting subsections of a configuration file, you can disconnect yourself from the GUI or CLI and 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 the configuration data before 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 fails and alerts are 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. The encoding attribute is specified in the file whenever you issue the `showconfig`, `saveconfig`, or `mailconfig` command:

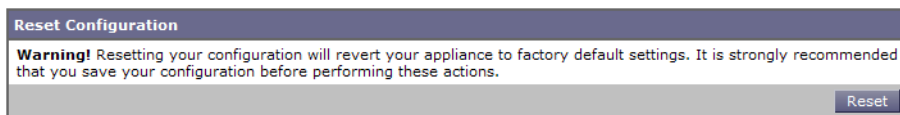
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

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. Save your configuration prior to resetting it. Resetting the configuration via the **Reset** button in the GUI is not supported in a clustering environment.

**Figure 12-41**     *Resetting the Configuration File*



See [Resetting to Factory Defaults](#), page 12-6.

## CLI Commands for Configuration Files

The following commands enable you to manipulate the configuration files:

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `resetconfig` (see [Resetting to Factory Defaults](#), page 12-6)
- `publishconfig`
- `backupconfig`

### 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 leaves any password field blank. You can choose not to include passwords if you are concerned about security breaches. However, configuration files without passwords fail when loaded using the `loadconfig` command. See [Note About Loading Passwords for Log Subscriptions](#), page 12-109.

**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: Cisco 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 on the Security Management appliance stores and saves all of the configuration master files (ESA and WSA) with a unique filename to the configuration directory.

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

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

The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration directory.

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

## The loadconfig Command

Use the `loadconfig` command to load new configuration information into the Cisco IronPort appliance. You can load information using 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 12-105](#) for more information.

## The publishconfig Command

Use the `publishconfig` command to publish changes a configuration master. The syntax is as follows:

```
publishconfig config_master [job_name] [host_list | host_ip]
```

where *config\_master* is a supported Configuration Master, as listed in [Table 2-5](#) of the [SMA Compatibility Matrix](#), page 2-32. This keyword is required. The keyword *job\_name* is optional and will be generated if it is not specified.

The keyword *host\_list* is a list of host names or IP addresses for WSA appliances to be published, and will be published to all hosts assigned to the configuration master if not specified. The optional *host\_ip* can be multiple host IP addresses, each separated by a comma.

To verify that the `publishconfig` command was successful, check the `smad_logs` file. You can also verify that the publish history was successful from the Security Management appliance GUI by choosing **Web > Utilities > Web Appliance Status**. From this page choose the web appliance that you want the publish history details. Additionally, you can go the Publish History page: **Web > Utilities > Publish > Publish History**.

## The backupconfig Command

Use the `backupconfig` command to copy the active dataset from the ‘source’ appliance to a ‘target’ Security Management appliance with minimum disruption on the originating ‘source’ Security Management appliance.

For more information on this command, the usage, and backing up your dataset, see [“Backing Up Your Security Management Appliance”](#) section on page 12-8.

## Uploading Configuration Changes Using 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 press Ctrl-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 gateway information. (For more information, see [Understanding the System Setup Wizard, page 2-9](#).) 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> commit
```

Please enter some comments describing your changes:

```
[> pasted new configuration file and changed default settings
```

## Managing Disk Usage

Use the **Management Appliance > System Administration > Disk Management** page to view the amount of disk space allocated to each of the Security Management appliance's monitoring services — the Cisco IronPort Spam Quarantine, centralized reporting, centralized web tracking, and centralized email tracking. The sum of the disk quotas for the four services is the total amount of disk space allocated for monitoring services on the appliance, as shown in the following example.

Figure 12-42 Disk Management Page

Data Disk Management

| Centralized Service Quotas and Usage |                    |     |                                     |
|--------------------------------------|--------------------|-----|-------------------------------------|
| Service                              | Current Disk Usage |     | Current Disk Quota                  |
| Spam Quarantine                      | 0 G                |     | 40 G                                |
| Centralized Reporting                | 0 G                |     | 20 G                                |
| Centralized Web Tracking*            | 0 G                |     | 80 G                                |
| Centralized Email Tracking           | 0 G                |     | 80 G                                |
| Total Space Used:                    |                    | 0 G | Total Space Allocated: 180G of 180G |
| <a href="#">Edit Disk Quotas...</a>  |                    |     |                                     |

\*Some data is used for web detail reports

# Maximum Disk Space Available

Table 12-7 shows the maximum amount of disk space available for centralized reporting, centralized email and web tracking, and Cisco IronPort Spam Quarantine (ISQ) on the specific Security Management appliances. All sizes are listed in Gigabytes (GB).

Table 12-7 Maximum Disk Space Available.

| Disk Space Available                            | Hardware Platform |      |      |      |      |       |       |       |       |
|-------------------------------------------------|-------------------|------|------|------|------|-------|-------|-------|-------|
|                                                 | M160              | M600 | M650 | M660 | M670 | M1000 | M1050 | M1060 | M1070 |
| Reporting + Email Tracking + ISQ + Web Tracking | 180               | 186  | 186  | 450  | 700  | 405   | 405   | 800   | 1500  |
| ISQ Maximums                                    | 70                | 100  | 100  | 150  | 150  | 200   | 200   | 265   | 265   |



Note

Unlike reporting (which is just counters) and tracking (which stores limited amounts of header information), the ISQ actually stores the entire message bodies of quarantined messages on the hard disk, and therefore uses significantly more space per message than the other features. Because of this significant space usage, handing over all of your hard drive to ISQ can occasionally lead to locking up the machine. Because of this, the ISQ disk quota has stricter limitations than just the available disk space.

## Editing Disk Quotas

You can change the amount of disk space allocated for each service by clicking on **Edit Disk Quotas**. For example, if you notice that centralized tracking consistently requires more hard drive space than centralized reporting and the Cisco IronPort Spam Quarantine, you can adjust the amount of space allocated to the centralized tracking service. As long as the quota you are setting the Web Reporting and Tracking to is larger than the currently used disk space, you will not lose any Web Reporting and Tracking data.

If you change the allocation so that the new allocation is smaller than the current space occupied, then the oldest data gets deleted until all data fits within the new allocation amount. If the allocation is set to zero, no data is retained.

If the **Enable** checkbox is selected for centralized reporting on the Web Security appliance, and there is no disk space allocated for this action, centralized web reporting will not work until disk space is allocated. See [Enabling and Disabling Centralized Web Reporting on a Security Management Appliance, page 3-5](#), for more information on editing this setting.

## Reallocating Monitoring Service Disk Quotas

To change the amount of disk space allocated to each monitoring service:

- 
- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > Disk Management**
  - Step 2** Click **Edit Disk Quotas**.
  - Step 3** On the **Edit Disk Quotas** page, enter the amount of disk space (in gigabytes) allocated to each service.

For a particular service, you can enter a value from 0 up to the total amount of disk space. The totaled disk quotas for all four services must add up to the total number of gigabytes displayed. For example, if the total disk space available is 200 GB and you allocate 25 GB for centralized reporting, 10 GB for the Cisco IronPort Spam Quarantine, and 35 GB for centralized email tracking, then you may allocate up to 130 GB for centralized web tracking to maintain the total of 200 GB for disk availability.

- Step 4** Click **Submit**.

**Step 5** In the confirmation dialog box, click **Set New Quotas**.

**Step 6** Click **Commit** to commit your changes.

---





# CHAPTER 13

## Logging

---

An important feature of the Security Management appliance is its logging capabilities. AsyncOS generates various types of logs that record different kinds of information. The Security Management appliance provides these logs as an important resource for system information outside the command line interface (CLI). Log files record regular operations, as well as exceptions, from various components of the system. This information can be valuable when monitoring the Cisco IronPort appliance. You can also use the logs for troubleshooting and evaluating performance.

This chapter contains the following sections:

- [Overview, page 13-1](#)
- [Log Characteristics, page 13-8](#)
- [Log Subscriptions, page 13-36](#)

## Overview

Logs are an efficient method of gathering critical information about the day-to-day operations of AsyncOS. Log files record information about activity on the Cisco IronPort appliance. The information varies depending on the type of log file. For example, Cisco IronPort Spam Quarantine logs record information about the quarantine, and Cisco IronPort Mail Text logs record information about email that traverses the appliance.

Most logs are recorded in plain text (ASCII) format; however, tracking logs are recorded in binary format for resource efficiency. The ASCII text information is readable in any text editor.

## Logging Versus Reporting

Use logging data to debug message flow, reveal basic day-to-day operational information such as FTP connection details, HTTP log files, and for compliance archiving.

You can access this logging data directly on the Email Security appliance or send it to any external FTP server for archival or reading. You can either FTP to the appliance to access the logs or push the plain text logs to an external server for backup purposes.

To view reporting data, use the Report pages on the appliance GUI. You cannot access the underlying data in any way, and this data cannot be sent to anything but a Security Management appliance.



### Note

---

The Security Management appliance pulls information for all reporting and tracking with the exception of Cisco IronPort Spam Quarantine (ISQ) data. The ISQ data is pushed from the ESA.

---

## Log Types

A log subscription associates a log type with a name, a logging level, and other characteristics such as file size and destination information. Multiple subscriptions for all log types, except configuration history logs, are permitted. The log type determines the data that are recorded in the log. You select the log type when you create a log subscription. See [Log Subscriptions, page 13-36](#) for more information.

AsyncOS generates the following log types:

**Table 13-1 Log Types**

| Log Type                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configuration History Logs</b>              | Configuration history logs record the following information: What changes were made on the Security Management appliance, and when were the changes made? A new configuration history log is created each time a user commits a change.                                                                                                                                                                                                                                        |
| <b>CLI Audit Logs</b>                          | The CLI audit logs record all CLI activity on the system.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>FTP Server Logs</b>                         | FTP logs record information about the FTP services enabled on the interface. Connection details and user activity are recorded.                                                                                                                                                                                                                                                                                                                                                |
| <b>HTTP Logs</b>                               | HTTP logs record information about the HTTP and secure HTTP services enabled on the interface. Because the graphical user interface (GUI) is accessed through HTTP, the HTTP logs are essentially the GUI equivalent of the CLI audit logs. Session data (for example, new sessions and expired sessions) are recorded, as well as the pages accessed in the GUI.                                                                                                              |
| <b>Cisco IronPort Spam Quarantine Logs</b>     | Cisco IronPort Spam Quarantine logs record actions associated with the Cisco IronPort Spam Quarantine processes.                                                                                                                                                                                                                                                                                                                                                               |
| <b>Cisco IronPort Spam Quarantine GUI Logs</b> | Cisco IronPort Spam Quarantine GUI logs record actions associated with the Cisco IronPort Spam Quarantine GUI, such as quarantine configuration through the GUI, end user authentication, and end user actions (for example, releasing email).                                                                                                                                                                                                                                 |
| <b>Cisco IronPort Text Mail Logs</b>           | Text mail logs record information about the operations of the email system (for example, message receiving, message delivery attempts, opening and closing connections, bouncing messages, and so forth).<br><br>For important information about when attachment names are included in mail logs, see <a href="#">Enabling and Disabling Centralized Email Tracking on a Security Management Appliance, page 3-6</a> and <a href="#">Tracking Service Overview, page 6-1</a> . |
| <b>NTP Logs</b>                                | NTP logs record the conversation between the appliance and any configured Network Time Protocol (NTP) servers. For information about configuring NTP servers, see <a href="#">Configuring the System Time, page 12-98</a> .                                                                                                                                                                                                                                                    |
| <b>Reporting Logs</b>                          | Reporting logs record actions associated with the processes of the centralized reporting service.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Reporting Query Logs</b>                    | Reporting query logs record actions associated with the reporting queries that are run on the appliance.                                                                                                                                                                                                                                                                                                                                                                       |

**Table 13-1 Log Types (continued)**

| Log Type                       | Description                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Safelist/Blocklist Logs</b> | Safelist/blocklist logs record data about the safelist/blocklist settings and database.                                                                                                                                                                                                                                                          |
| <b>SMA Logs</b>                | SMA logs record actions associated with general Security Management appliance processes, not including the processes of the centralized reporting, centralized tracking, and Cisco IronPort Spam Quarantine services.                                                                                                                            |
| <b>Status Logs</b>             | Status logs record 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. |
| <b>System Logs</b>             | System logs record the following: boot information, DNS status information, and comments users typed using the <code>commit</code> command. System logs are useful for troubleshooting the state of the appliance.                                                                                                                               |
| <b>Tracking Logs</b>           | Tracking logs record actions associated with the processes of the tracking service. Tracking logs are a subset of the mail logs.                                                                                                                                                                                                                 |

## Log Type Comparison

Table 13-2 summarizes the characteristics of each log type.

**Table 13-2 Log Type Comparison**

|                            |               |           |                  |                    |                | Contains                    |                               |                      |                         |                         |                           |
|----------------------------|---------------|-----------|------------------|--------------------|----------------|-----------------------------|-------------------------------|----------------------|-------------------------|-------------------------|---------------------------|
|                            | Transactional | Stateless | Recorded as Text | Recorded as Binary | Header Logging | Periodic Status Information | Message Receiving Information | Delivery Information | Individual Hard Bounces | Individual Soft Bounces | Configuration Information |
| Configuration History Logs | •             |           | •                |                    |                |                             |                               |                      |                         |                         | •                         |
| CLI Audit Logs             | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |

Table 13-2 Log Type Comparison (continued)

|                                    | Contains      |           |                  |                    |                |                             |                               |                      |                         |                         |                           |
|------------------------------------|---------------|-----------|------------------|--------------------|----------------|-----------------------------|-------------------------------|----------------------|-------------------------|-------------------------|---------------------------|
|                                    | Transactional | Stateless | Recorded as Text | Recorded as Binary | Header Logging | Periodic Status Information | Message Receiving Information | Delivery Information | Individual Hard Bounces | Individual Soft Bounces | Configuration Information |
| FTP Server Logs                    | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| HTTP Logs                          | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Cisco IronPort Spam Quarantine     | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Cisco IronPort Spam Quarantine GUI | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Cisco IronPort Text Mail Logs      | •             |           | •                |                    | •              | •                           | •                             | •                    | •                       | •                       |                           |
| NTP Logs                           | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Reporting Logs                     | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Reporting Query Logs               | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Safelist/Blocklist Logs            | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| SMA Logs                           | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Status Logs                        |               | •         | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| System Logs                        | •             |           | •                |                    |                | •                           |                               |                      |                         |                         |                           |
| Tracking Logs                      | •             |           |                  | •                  | •              |                             | •                             | •                    | •                       | •                       |                           |

## Log Retrieval

Log files can be retrieved with the file transfer protocols described in [Table 13-3](#). You set the protocol when you create or edit a log subscription in the GUI, or by using the `logconfig` command in the CLI.

**Table 13-3**      **Log Transfer Protocols**

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FTP Poll</b>    | With this type of file transfer, a remote FTP client accesses the Cisco IronPort appliance to retrieve log files by using the username and password of an administrator-level or operator-level user. When configuring a log subscription to use the FTP poll method, you must supply the maximum number of log files to retain. When the maximum number is reached, the system deletes the oldest file.                                          |
| <b>FTP Push</b>    | With this type of file transfer, the Cisco IronPort appliance 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 the configured rollover schedule.                                                                                                                                         |
| <b>SCP Push</b>    | With this type of file transfer, the Cisco IronPort appliance 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 the configured rollover schedule.                                             |
| <b>Syslog Push</b> | With this type of file transfer, the Cisco IronPort appliance sends log messages to a remote syslog server. This method conforms to RFC 3164. You must submit a hostname for the syslog server and 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 preselected in the drop-down menu. Only text-based logs can be transferred using syslog push. |

## Filename and Directory Structure

AsyncOS creates a directory for each log subscription based on the log name specified in the log subscription. The filenames of logs in the directory consist of the filename specified in the log subscription, the timestamp when the log file was started, and a single-character status code. The following example shows the convention for the directory and filename:

```
/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>
```

Status codes may be `.c` (signifying “current”) or `.s` (signifying “saved”). You should only transfer log files with the saved status.

## Log Rollover and Transfer Schedule

Log subscriptions create logs and roll over (transfer) the log files based on the following configuration limits: maximum file size and maximum time. When either limit is reached, the log file is rolled over. Log subscriptions based on the FTP poll transfer mechanism create files and store them in the FTP directory on the Cisco IronPort appliance until they are retrieved or until the system needs more space for log files.

## Logs Enabled by Default

The Security Management appliance is preconfigured with the following log subscriptions enabled.

**Table 13-4**      *Preconfigured Log Subscriptions*

| Log Name          | Log Type                                | Retrieval Method |
|-------------------|-----------------------------------------|------------------|
| cli_logs          | CLI Audit Logs                          | FTP Poll         |
| euq_logs          | Cisco IronPort Spam Quarantine Logs     | FTP Poll         |
| euqgui_logs       | Cisco IronPort Spam Quarantine GUI Logs | FTP Poll         |
| gui_logs          | HTTP Logs                               | FTP Poll         |
| mail_logs         | Cisco IronPort Text Mail Logs           | FTP Poll         |
| reportd_logs      | Reporting Logs                          | FTP Poll         |
| reportqueryd_logs | Reporting Query Logs                    | FTP Poll         |
| slbld_logs        | Safelist/Blocklist Logs                 | FTP Poll         |
| smad_logs         | SMA Logs                                | FTP Poll         |
| system_logs       | System Logs                             | FTP Poll         |
| trackerd_logs     | Tracking Logs                           | FTP Poll         |

All preconfigured log subscriptions have the logging level set to Information. For more information about log levels, see [Setting the Log Level, page 13-38](#).

You can configure additional log subscriptions depending on the license keys that you have applied. For information about creating and editing log subscriptions, see [Log Subscriptions](#), page 13-36.

## Log Characteristics

This section describes the following log types:

- [Using Configuration History Logs](#), page 13-9
- [Using CLI Audit Logs](#), page 13-10
- [Using FTP Server Logs](#), page 13-11
- [Using HTTP Logs](#), page 13-12
- [Using Cisco IronPort Spam Quarantine Logs](#), page 13-14
- [Using Cisco IronPort Spam Quarantine GUI Logs](#), page 13-15
- [Using Cisco IronPort Text Mail Logs](#), page 13-15
- [Using NTP Logs](#), page 13-25
- [Using Reporting Logs](#), page 13-26
- [Using Reporting Query Logs](#), page 13-27
- [Using Safelist/Blocklist Logs](#), page 13-29
- [Using SMA Logs](#), page 13-30
- [Using Status Logs](#), page 13-31
- [Using System Logs](#), page 13-35
- [Understanding Tracking Logs](#), page 13-36

## Timestamps in Log Files

The following log files include the beginning and ending date of the log itself, the version of AsyncOS, and the GMT offset (provided in seconds at the beginning of the log):

- Mail log
- Safelist/blocklist log



- System log

## 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-D000000

```
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>
```

# Using CLI Audit Logs

Table 13-5 describes the statistics recorded in CLI audit logs.

**Table 13-5      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 that was entered, the CLI output (including menus, lists, and so forth), and the prompt that appears. |

## 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=====
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 FTP Server Logs

[Table 13-6](#) describes the statistics recorded in FTP server logs.

**Table 13-6** *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, and so forth). |

## 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 HTTP Logs

[Table 13-7](#) describes the statistics recorded in HTTP logs

**Table 13-7 Statistics Recorded in HTTP Logs.**

| Statistic | Description                           |
|-----------|---------------------------------------|
| Timestamp | Time that the bytes were transmitted. |
| ID        | Session ID.                           |
| req       | IP address of machine connecting.     |

| Statistic      | Description                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------|
| <b>user</b>    | Username of user connecting.                                                                                  |
| <b>Message</b> | Information regarding the actions performed. May include GET or POST commands or system status, and so forth. |

## HTTP Log Example

In this example, the HTTP log shows the admin user's interaction with the GUI (for example, running the System Setup Wizard).

```

Wed Sep  8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting
to https port 443

Wed Sep  8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep  8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep  8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep  8 11:17:24 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg POST /system_administration/system_setup_wizard
HTTP/1.1 303

Wed Sep  8 11:17:25 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /system_administration/ssw_done HTTP/1.1 200

Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep  8 11:18:45 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin
&height=190 HTTP/1.1 200

Wed Sep  8 11:18:46 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipie
nts&in&height=190 HTTP/1.1 200

Wed Sep  8 11:18:49 2004 Info: req:10.10.10.14 user:admin
id:iaCkEh2h5rZknQarAecg GET /monitor/quarantines HTTP/1.1 200

```

## Using Cisco IronPort Spam Quarantine Logs

Table 13-8 describes the statistics recorded in Cisco IronPort Spam Quarantine logs.

**Table 13-8** *Cisco IronPort Spam Quarantine Log Statistics*

| Statistic | Description                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------|
| Timestamp | Time that the bytes were transmitted.                                                                 |
| Message   | The message consists of actions taken (messages quarantined, released from quarantine, and so forth). |

### Cisco IronPort Spam Quarantine Log Example

In this example, the log shows two messages (MID 8298624 and MID 8298625) 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 Cisco IronPort Spam Quarantine GUI Logs

[Table 13-9](#) shows the statistics recorded in Cisco IronPort Spam Quarantine GUI logs.

**Table 13-9** *Cisco IronPort Spam Quarantine GUI Log Statistics*

| Statistic | Description                                                                         |
|-----------|-------------------------------------------------------------------------------------|
| Timestamp | Time that the bytes were transmitted.                                               |
| Message   | The message consists of actions taken, including user authentication, and so forth. |

### Cisco IronPort Spam Quarantine GUI Log Example

In this example, the log shows a successful authentication, login, and logout:

**Table 13-10** *Cisco IronPort Spam Quarantine GUI Log Example*

```
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 Cisco IronPort Text Mail Logs

These 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.

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. See [Enabling and Disabling Centralized Email Tracking on a Security Management Appliance](#), page 3-6 and [Tracking Service Overview](#), page 6-1.

Table 13-11 shows the information displayed in text mail logs.

**Table 13-11 Text Mail Log Statistics**

| Statistic    | Description                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ICID</b>  | Injection Connection ID. This is a numerical identifier for an individual SMTP connection to the system. A single message or thousands of individual messages can be sent over one SMTP connection to the system.                             |
| <b>DCID</b>  | Delivery Connection ID. This is a numerical identifier for an individual SMTP connection to another server, for delivery of one to thousands of messages, each with some or all of its RIDs being delivered in a single message transmission. |
| <b>RCID</b>  | 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.                       |
| <b>MID</b>   | Message ID: Use this to track messages as they flow through the logs.                                                                                                                                                                         |
| <b>RID</b>   | Recipient ID. Each message recipient is assigned an ID.                                                                                                                                                                                       |
| <b>New</b>   | New connection initiated.                                                                                                                                                                                                                     |
| <b>Start</b> | New message started.                                                                                                                                                                                                                          |

## Sample

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 13-12 Text Mail Log Detail**

|          |                                                                                                                                                |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b> | 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 |
| <b>2</b> | Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5                                                                                              |
| <b>3</b> | Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>                                                                      |
| <b>4</b> | Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>                                                                    |



**Table 13-12**     **Text Mail Log Detail (continued)**

|           |                                                                                          |
|-----------|------------------------------------------------------------------------------------------|
| <b>5</b>  | Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>        |
| <b>6</b>  | Mon Apr 17 19:59:59 2003 Info: ICID 5 close                                              |
| <b>7</b>  | Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25 |
| <b>8</b>  | Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]                    |
| <b>9</b>  | Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]                      |
| <b>10</b> | Mon Mar 31 20:11:03 2003 Info: DCID 8 close                                              |

Use [Table 13-13](#) as a guide to reading the previous log file.

**Table 13-13**     **Detail of Text Mail Log Example**

| Line Number | Description                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b>    | 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. |
| <b>2</b>    | The message is assigned a Message ID (MID) of “6” after the MAIL FROM command is issued from the client.                                                                                                   |
| <b>3</b>    | The sender address is identified and accepted.                                                                                                                                                             |
| <b>4</b>    | The recipient is identified and assigned a Recipient ID (RID) of “0.”                                                                                                                                      |
| <b>5</b>    | MID 5 is accepted, written to disk, and acknowledged.                                                                                                                                                      |
| <b>6</b>    | Receiving is successful and the receiving connection closes.                                                                                                                                               |
| <b>7</b>    | 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.                                                                            |
| <b>8</b>    | The message delivery starts to RID “0.”                                                                                                                                                                    |
| <b>9</b>    | Delivery is successful for MID 6 to RID “0.”                                                                                                                                                               |
| <b>10</b>   | The delivery connection closes.                                                                                                                                                                            |

## Examples of Text Mail Log Entries

The following examples show log entries based on various cases.

## Message Receiving

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 Example

```
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 with Ultimately Successful Delivery Example

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 (scanconfig)

When using the `scanconfig` command to determine behavior when a message could not be deconstructed into its component parts (when removing attachments) as with this prompt:

If a message could not be deconstructed into its component parts in order to remove specified attachments, the system should:

1. Deliver
2. Bounce

3. Drop

[3]>

the following is the indication in the mail logs:

*With scanconfig set to deliver if message could not be decomposed.*

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

*With scanconfig set to drop if message could not be decomposed.*

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.

## Generated or Rewritten Messages

Some functions, such as rewrite/redirect actions (`alt-rcpt-to` filters, anti-spam `rcpt rewrite`, `bcc()` actions, anti-virus redirections, and so forth), create new messages. When looking through the logs, you might need to check the results and add in additional 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'
```



#### Note

---

“Rewritten” entries can appear after lines in the log indicating use of the new MID.

---

## Sending a Message 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.pimailer44.DumpShot.2@email.  
chase.com>'
```

```
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream  
home - Now make it a reality'
```

```
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from  
<HLD@chasehf.bfi0.com>
```

```
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for  
per-recipient policy DEFAULT in the inbound table
```



```

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam
suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine

Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative

Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery

Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID
2317877 to local Cisco 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 NTP Logs

Table 13-14 shows the statistics recorded in NTP logs.

**Table 13-14 Statistics Recorded in NTP Logs**

| 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 Reporting Logs

[Table 13-15](#) shows the statistics recorded in reporting logs.

**Table 13-15**      **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 13-16 shows the statistics recorded in reporting query logs.

**Table 13-16**      *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 Safelist/Blocklist Logs

Table 13-17 shows the statistics recorded in safelist/blocklist logs.

**Table 13-17 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 SMA Logs

Table 13-18 shows the statistics recorded in SMA logs.

**Table 13-18**      **SMA Log Statistics**

| Statistic | Description                                                                         |
|-----------|-------------------------------------------------------------------------------------|
| Timestamp | Time that the bytes were transmitted.                                               |
| Message   | The message consists of actions taken, including user authentication, and so forth. |

In this example, the SMA log shows the centralized tracking service downloading tracking files from an Email Security appliance, and it shows the centralized reporting service downloading reporting files from an Email Security appliance.

```

Wed Oct 3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN
downloading from 172.29.0.17 - /export/tracki

```

```

ng/tracking.@20071003T202244Z_20071003T202544Z.s

```

```

Wed Oct 3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN
downloading from 172.29.0.15 - /export/tracki

```

```

ng/tracking.@20071003T202443Z_20071003T202743Z.s

```

```

Wed Oct 3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN
downloading from 172.29.0.17 - /export/tracki

```

```

ng/tracking.@20071003T202544Z_20071003T202844Z.s

```

```
Wed Oct 3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN
downloading from 172.29.0.15 - /export/tracki

ng/tracking.@20071003T202743Z_20071003T203043Z.s

Wed Oct 3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN
downloading from 172.29.0.15 - /reporting/ou

tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz

Wed Oct 3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN
downloading from 172.29.0.17 - /export/tracki

ng/tracking.@20071003T202844Z_20071003T203144Z.s

Wed Oct 3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN
downloading from 172.29.0.17 - /reporting/ou

tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz

Wed Oct 3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN
downloading from 172.29.0.15 - /export/tracki

ng/tracking.@20071003T203043Z_20071003T203343Z.s
```

## Using 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 13-19 shows the status log labels and the matching system statistics.

**Table 13-19 Status Log Statistics**

| Statistic         | Description                     |
|-------------------|---------------------------------|
| <b>CPULd</b>      | CPU utilization.                |
| <b>DskIO</b>      | Disk I/O utilization.           |
| <b>RAMUtil</b>    | RAM utilization.                |
| <b>QKUsd</b>      | Queue kilobytes used.           |
| <b>QKFre</b>      | Queue kilobytes free.           |
| <b>CrtMID</b>     | Message ID (MID).               |
| <b>CrtICID</b>    | Injection connection ID (ICID). |
| <b>CRTDCID</b>    | Delivery connection ID (DCID).  |
| <b>InjMsg</b>     | Injected messages.              |
| <b>InjRcp</b>     | Injected recipients.            |
| <b>GenBncRcp</b>  | Generated bounce recipients.    |
| <b>RejRcp</b>     | Rejected recipients.            |
| <b>DrpMsg</b>     | Dropped messages.               |
| <b>SftBncEvt</b>  | Soft bounced events.            |
| <b>CmpRcp</b>     | Completed recipients.           |
| <b>HrdBncRcp</b>  | Hard bounced recipients.        |
| <b>DnsHrdBnc</b>  | DNS hard bounces.               |
| <b>5XXHrdBnc</b>  | 5XX hard bounces.               |
| <b>FltrHrdBnc</b> | Filter hard bounces.            |
| <b>ExpHrdBnc</b>  | Expired hard bounces.           |
| <b>OtrHrdBnc</b>  | Other hard bounces.             |
| <b>DlvRcp</b>     | Delivered recipients.           |
| <b>DelRcp</b>     | Deleted recipients.             |
| <b>GlbUnsbHt</b>  | Global unsubscribe hits.        |



**Table 13-19 Status Log Statistics (continued)**

| <b>Statistic</b>  | <b>Description</b>                                                                                                             |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>ActvRcp</b>    | Active recipients.                                                                                                             |
| <b>UnatmptRcp</b> | Unattempted recipients.                                                                                                        |
| <b>AtmptRcp</b>   | Attempted recipients.                                                                                                          |
| <b>CrtCncIn</b>   | Current inbound connections.                                                                                                   |
| <b>CrtCncOut</b>  | Current outbound connections.                                                                                                  |
| <b>DnsReq</b>     | DNS requests.                                                                                                                  |
| <b>NetReq</b>     | Network requests.                                                                                                              |
| <b>CchHit</b>     | Cache hits.                                                                                                                    |
| <b>CchMis</b>     | Cache misses.                                                                                                                  |
| <b>CchEct</b>     | Cache exceptions.                                                                                                              |
| <b>CchExp</b>     | Cache expired.                                                                                                                 |
| <b>CPUTTm</b>     | Total CPU time used by the application.                                                                                        |
| <b>CPUETm</b>     | Elapsed time since the application started.                                                                                    |
| <b>MaxIO</b>      | Maximum disk I/O operations per second for the mail process.                                                                   |
| <b>RamUsd</b>     | Allocated memory in bytes.                                                                                                     |
| <b>SwIn</b>       | Memory swapped in.                                                                                                             |
| <b>SwOut</b>      | Memory swapped out.                                                                                                            |
| <b>SwPgIn</b>     | Memory paged in.                                                                                                               |
| <b>SwPgOut</b>    | Memory paged out.                                                                                                              |
| <b>MMLen</b>      | Total number of messages in the system.                                                                                        |
| <b>DstInMem</b>   | Number of destination objects in memory.                                                                                       |
| <b>ResCon</b>     | Resource conservation tarpit value. Acceptance of incoming mail is delayed by this number of seconds due to heavy system load. |
| <b>WorkQ</b>      | Number of messages currently in the work queue.                                                                                |

**Table 13-19      Status Log Statistics (continued)**

| <b>Statistic</b> | <b>Description</b>                                                                                                       |
|------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>QuarMsgs</b>  | Number of individual messages in the system quarantine (messages present in multiple quarantines are counted only once). |
| <b>QuarQKUsd</b> | Kilobytes used by system quarantine messages.                                                                            |
| <b>LogUsd</b>    | Percent of log partition used.                                                                                           |
| <b>CASELd</b>    | Percent CPU used by CASE scanning.                                                                                       |
| <b>TotalLd</b>   | Total CPU consumption.                                                                                                   |
| <b>LogAvail</b>  | Amount of disk space available for log files.                                                                            |
| <b>EuQ</b>       | Number of messages in the Cisco IronPort Spam Quarantine.                                                                |
| <b>EuQRls</b>    | 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 SftBncEvt 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 System Logs

Table 13-20 shows the statistics recorded in system logs.

**Table 13-20**      **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: 6.0.0-206 SN: XXXXXXXXXXXXX-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.
```

## 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 IronPort. The conversion tools are located at the following URL: <http://tinyurl.com/3c518r>.

## Log Subscriptions

This section contains the following topics:

- [Configuring Log Subscriptions, page 13-37](#)
- [Creating a Log Subscription in the GUI, page 13-39](#)
- [Configuring Global Settings for Logging, page 13-41](#)
- [Rolling Over Log Subscriptions, page 13-45](#)
- [Configuring Host Keys, page 13-48](#)

## Configuring Log Subscriptions

Log subscriptions create the individual log files that are stored on a Cisco IronPort appliance or remotely. A log subscription is either pushed (delivered to another computer) or polled (retrieved from the appliance). Generally, log subscriptions have the following attributes:

**Table 13-21** Log File Attributes

| Attribute         | Description                                                                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Type          | Defines the type of information recorded and the format of the log subscription. For more information, see <a href="#">Log Types, page 13-2</a> .                                                 |
| Name              | Descriptive name of log subscription that you provide for your future reference.                                                                                                                  |
| Log Level         | Level of detail for each log subscription.                                                                                                                                                        |
| Retrieval Method  | Method used to transfer the log files from the Cisco IronPort appliance.                                                                                                                          |
| Log Filename      | Physical name of the file when it is written to disk. If the system includes multiple Cisco IronPort appliances, use a unique log filename to identify the appliance that generated the log file. |
| Maximum File Size | Maximum size that the file can reach before it rolls over.                                                                                                                                        |

Use the Management Appliance > System Administration > Log Subscriptions page (or the `logconfig` command in the CLI) to configure a log subscription. You are prompted for the log type, as shown in [Log Types, page 13-2](#). For most log types, you are also asked to select a *log level* for the log subscription.



### Note

Configuration history logs only: If you anticipate loading configurations from the configuration history logs, be aware that you cannot load configurations containing masked passwords. On the Management Appliance > System Administration > Log Subscriptions page, select Yes when prompted whether you want to include passwords in the log. If you are using the `logconfig` command in the CLI, type `y` when prompted.

## Setting the Log Level

Log levels determine the amount of information delivered in a log. Logs can have one of five levels of detail. A detailed log-level setting creates larger log files and has a greater impact on system performance than an abbreviated log-level setting. A detailed log-level setting includes all the messages contained in the abbreviated log-level settings, plus additional messages. As the level of detail increases, system performance decreases.



### Note

You can specify different logging levels for each log type.

**Table 13-22 Log Levels**

| Log Level          | Description                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Critical</b>    | Only errors are logged. This is the most abbreviated log-level setting. At this log level, you cannot monitor performance and important appliance activities; however, the log files do not reach maximum size as quickly as they do at a detailed log level. This log level is analogous to the syslog level Alert. |
| <b>Warning</b>     | All system errors and warnings are logged. At this log level, you cannot monitor performance and important appliance activities. The log files reach maximum size more quickly than they do at the Critical log level. This log level is analogous to the syslog level Warning.                                      |
| <b>Information</b> | Second-by-second operations of the system are logged. For example, connections opened and delivery attempts are logged. The Information level is the recommended setting for logs. This log level is analogous to the syslog level Info.                                                                             |
| <b>Debug</b>       | More detailed information is logged than at the Information log level. Use the Debug log level when you are troubleshooting an error. Use this setting temporarily, and then return to the default level. This log level is analogous to the syslog level Debug.                                                     |
| <b>Trace</b>       | All available information is logged. 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 analogous to the syslog level Debug.                                                                      |

## Creating a Log Subscription in the GUI

To create a log subscription:

- 
- Step 1** On the Management Appliance > System Administration > Log Subscriptions page, click **Add Log Subscription**. The New Log Subscription page appears.

Figure 13-1 Creating a New Log Subscription

## New Log Subscription

| Log Subscription   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Type:          | Select a log type...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Log Name:          | <input type="text"/><br><i>(will be used to name the log directory)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| File Name:         | <input type="text"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Maximum File Size: | 10M<br><i>(Add a trailing K or M to indicate size units)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Log Level:         | <input type="radio"/> Critical (The least detailed setting. Only errors are logged.)<br><input type="radio"/> Warning (All errors and warnings created by the system.)<br><input checked="" type="radio"/> Information (Captures the second-by-second operations of the system. Recommended.)<br><input type="radio"/> Debug (More specific data are logged to help debug specific problems.)<br><input type="radio"/> Trace (The most detailed setting, all information that can be is logged. Recommended for developers only.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Retrieval Method:  | <input checked="" type="radio"/> FTP on test28.eng<br><div>Maximum Number of Files: <input type="text" value="10"/></div> <input type="radio"/> FTP on Remote Server<br><div>Maximum Time Interval Between Transferring: <input type="text" value="3600"/> seconds</div> <div>FTP Host: <input type="text"/></div> <div>Directory: <input type="text"/></div> <div>Username: <input type="text"/></div> <div>Password: <input type="text"/></div> <input type="radio"/> SCP on Remote Server<br><div>Maximum Time Interval Between Transferring: <input type="text" value="3600"/> seconds</div> <div>Protocol: <input type="radio"/> SSH1 <input checked="" type="radio"/> SSH2</div> <div>SCP Host: <input type="text"/></div> <div>Directory: <input type="text"/></div> <div>Username: <input type="text"/></div> <div> <input type="checkbox"/> Enable Host Key Checking<br/> <input checked="" type="radio"/> Automatically Scan<br/> <input type="radio"/> Enter Manually<br/> <input type="text"/> </div> |

Cancel
Submit



- Step 2** Select a log type and enter the log name (for the log directory), as well as the name for the log file itself.
- Step 3** If applicable, specify the maximum file size and the log level.
- Step 4** (Configuration history logs only) Select whether to include passwords in the log.




---

**Note** You cannot load configurations containing masked passwords. If you anticipate loading configurations from the configuration history logs, select Yes to include passwords in the log.

---

- 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 Name column on the Log Subscriptions page. The Edit Log Subscription page appears.
- Step 2** Update the log subscription.
- Step 3** Submit and commit your changes.

## Configuring Global Settings for Logging

The system periodically records system metrics within text mail logs and status logs. Use the **Edit Settings** button in the Global Settings section of the Log Subscriptions page (or the `logconfig -> setup` command in the CLI) to configure:

- The amount of time, in seconds, that the system waits between recording metrics
- 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
- The headers that should be logged for each message

All Cisco IronPort logs optionally include the following three items:

- **Message-ID:** When this option is configured, every message will have its Message ID header logged, if it is available. This Message ID may have come from the received message or may have been generated by AsyncOS. For example:

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

- **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
```

White space, punctuation, and, in the case of the 250 response, the OK characters are stripped from the beginning of the string. Only white space 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 entry “Message MID accepted” would be logged if the remote host were another Cisco IronPort appliance.

- **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 on 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 text mail logs and the tracking 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 13-23 Log Headers**

|                    |                               |
|--------------------|-------------------------------|
| <b>Header name</b> | Name of the header            |
| <b>Value</b>       | Contents of the logged header |

For example, specifying “date, x-subject” as headers to be logged causes 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 by Using 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 appears.

**Figure 13-2** *Configuring Log Subscriptions Global Settings*

### Log Subscriptions Global Settings

| Edit Global Settings                |                                                                                                                                                                                                                             |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System metrics frequency:           | <input type="text" value="45"/> seconds                                                                                                                                                                                     |
| Logging Options:                    | <input checked="" type="checkbox"/> Message-ID headers in Mail Logs<br><input checked="" type="checkbox"/> Original subject header of each message<br><input checked="" type="checkbox"/> Remote response text in Mail Logs |
| Headers (Optional):                 | List any headers you want to record in the log files:<br><div>date</div> <div>x-subject</div>                                                                                                                               |
| <div>Cancel</div> <div>Submit</div> |                                                                                                                                                                                                                             |

- Step 2** Specify the system metrics 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 want to include in the logs.
- Step 4** Submit and commit your changes.

## Rolling Over Log Subscriptions

AsyncOS rolls over log files based on settings you make on the Log Subscriptions Global Settings page (or the `logconfig` command in the CLI). You can also roll log files on demand by clicking the **Rollover Now** button on the Log Subscriptions page or by using the `rollovernow` command. When AsyncOS rolls over a log file, it:

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

## Rolling Over Log Subscriptions Using the GUI

To roll over log subscriptions:

- 
- Step 1** On the Log Subscriptions page, select the check box to the right of the logs you want to roll over.
- Step 2** Optionally, select all logs for rollover by selecting the All check box.  
After one or more logs have been selected for rollover, the **Rollover Now** button is enabled.
- Step 3** Click the **Rollover Now** button to roll over the selected logs.

## Rolling Over Log Subscriptions via the CLI

Use the `rollovernow` command to roll over all log files at once or select a specific log file from a list.

# Viewing the Most Recent Log Entries in the GUI

You can view a log file via the GUI by clicking the log subscription in the Log Files column of the table on the Log Subscriptions page. When you click the link to the log subscription, you are prompted to enter your password. A listing of log files for that subscription then appears. You can click one of the log files to view it in your browser or to save it to disk. You must have the FTP service enabled on the Management interface to view logs in the GUI.

Figure 13-3 Viewing Log Files in the GUI

Log Subscriptions

| Configured Log Subscriptions            |                                   |                                                     |                                       |        |
|-----------------------------------------|-----------------------------------|-----------------------------------------------------|---------------------------------------|--------|
| <a href="#">Add Log Subscription...</a> |                                   |                                                     |                                       |        |
| Log Name                                | Type                              | Log Files                                           | All <input type="checkbox"/> Rollover | Delete |
| <a href="#">cli_logs</a>                | CLI Audit Logs                    | <a href="#">ftp://cyclone.eng/cli_logs</a>          | <input type="checkbox"/>              |        |
| <a href="#">euq_logs</a>                | IronPort Spam Quarantine Logs     | <a href="#">ftp://cyclone.eng/euq_logs</a>          | <input type="checkbox"/>              |        |
| <a href="#">euqgui_logs</a>             | IronPort Spam Quarantine GUI Logs | <a href="#">ftp://cyclone.eng/euqgui_logs</a>       | <input type="checkbox"/>              |        |
| <a href="#">gui_logs</a>                | HTTP Logs                         | <a href="#">ftp://cyclone.eng/gui_logs</a>          | <input type="checkbox"/>              |        |
| <a href="#">mail_logs</a>               | IronPort Text Mail Logs           | <a href="#">ftp://cyclone.eng/mail_logs</a>         | <input type="checkbox"/>              |        |
| <a href="#">reportd_logs</a>            | Reporting Logs                    | <a href="#">ftp://cyclone.eng/reportd_logs</a>      | <input type="checkbox"/>              |        |
| <a href="#">reportqueryd_logs</a>       | Reporting Query Logs              | <a href="#">ftp://cyclone.eng/reportqueryd_logs</a> | <input type="checkbox"/>              |        |
| <a href="#">slbld_logs</a>              | Safe/Block Lists Logs             | <a href="#">ftp://cyclone.eng/slbld_logs</a>        | <input type="checkbox"/>              |        |
| <a href="#">smad_logs</a>               | SMA Logs                          | <a href="#">ftp://cyclone.eng/smad_logs</a>         | <input type="checkbox"/>              |        |
| <a href="#">system_logs</a>             | System Logs                       | <a href="#">ftp://cyclone.eng/system_logs</a>       | <input type="checkbox"/>              |        |
| <a href="#">trackerd_logs</a>           | Tracking Logs                     | <a href="#">ftp://cyclone.eng/trackerd_logs</a>     | <input type="checkbox"/>              |        |

Note: To view log files via FTP you must enable the FTP service on the 'Management' Interface.

[Rollover Now](#)

# Viewing the Most Recent Entries in Logs (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. Press `Ctrl-C` to exit from the `tail` command.



Note

You cannot view configuration history logs by using the `tail` command. You must use FTP or SCP.

## Example

In the following example, the `tail` command is used to view the system log. The `tail` command also accepts the name of a log to view as a parameter, for example, `tail system_logs`.

```
Welcome to the Cisco IronPort M600 Messaging Gateway(tm) Appliance
```

```
example.srv> tail
```

```
Currently configured logs:
```

1. "cli\_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
  2. "euq\_logs" Type: "Cisco IronPort Spam Quarantine Logs" Retrieval: FTP Poll
  3. "euogui\_logs" Type: "Cisco IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
  4. "gui\_logs" Type: "HTTP Logs" Retrieval: FTP Poll
  5. "mail\_logs" Type: "Cisco IronPort Text Mail Logs" Retrieval: FTP Poll
  6. "reportd\_logs" Type: "Reporting Logs" Retrieval: FTP Poll
  7. "reportqueryd\_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
  8. "sblld\_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
  9. "smad\_logs" Type: "SMA Logs" Retrieval: FTP Poll
  10. "system\_logs" Type: "System Logs" Retrieval: FTP Poll
  11. "trackerd\_logs" Type: "Tracking Logs" Retrieval: FTP Poll
- ```
Enter the number of the log you wish to tail.  
  
[]> 10
```

```

Press Ctrl-C to stop.

Thu Sep 27 00:18:56 2007 Info: Begin Logfile

Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN:
001143583D73-FT9GP61

Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds

Thu Sep 27 00:18:47 2007 Info: System is coming up.

Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64]
Host is down' to '172.16.0.3' looking up 'downloads.cisco.com'

Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:

Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:

^Cexample.srv>

```

## 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” in the *Cisco IronPort AsyncOS for Email User Guide*.



The `hostkeyconfig` subcommand performs the following functions:

**Table 13-24 Managing Host Keys - List of Subcommands**

| Command            | Description                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>New</b>         | Add a new key.                                                                                                                                                                                                                                 |
| <b>Edit</b>        | Modify an existing key.                                                                                                                                                                                                                        |
| <b>Delete</b>      | Delete an existing key.                                                                                                                                                                                                                        |
| <b>Scan</b>        | Automatically download a host key.                                                                                                                                                                                                             |
| <b>Print</b>       | Display a key.                                                                                                                                                                                                                                 |
| <b>Host</b>        | Display system host keys. This is the value to place in the remote system's "known_hosts" file.                                                                                                                                                |
| <b>Fingerprint</b> | Display system host key fingerprints.                                                                                                                                                                                                          |
| <b>User</b>        | Display the public key of the system account that pushes the logs to the remote machine. This is the same key that appears 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, the commands scan 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**





# APPENDIX **A**

## Accessing the Appliance

You can access any IP interface you create on the appliance through a variety of services.

By default, the following services are either enabled or disabled on each interface:

**Table A-1**      *Services Enabled by Default on IP Interfaces*

|         |              | Enabled by default?  |                              |
|---------|--------------|----------------------|------------------------------|
| Service | Default Port | Management Interface | New IP Interfaces You Create |
| FTP     | 21           | No                   | No                           |
| Telnet  | 23           | Yes                  | No                           |
| SSH     | 22           | Yes                  | No                           |
| HTTP    | 80           | Yes                  | No                           |
| HTTPS   | 443          | Yes                  | No                           |

## IP Interfaces

An IP interface contains the network configuration data needed for an individual connection to the network. You can configure multiple IP interfaces to a physical Ethernet interface. You can also configure access to the Cisco IronPort Spam Quarantine via an IP interface. For email delivery and Virtual Gateways, each IP interface acts as one Virtual Gateway address with a specific IP address and hostname. You can also “join” interfaces into distinct groups (via the CLI), and the system will cycle through these groups when delivering email. Joining or

grouping Virtual Gateways is useful for load-balancing large email campaigns across several interfaces. You can also create VLANs, and configure them just as you would any other interface (via the CLI). For more information, see the “Advanced Networking” chapter in the *Cisco IronPort AsyncOS for Email Advanced User Guide*.

Figure A-1      IP Interfaces Page

IP Interfaces

| Network Interfaces and IP Addresses |                |               |        |
|-------------------------------------|----------------|---------------|--------|
| Add IP Interface...                 |                |               |        |
| Name                                | IP Address     | Hostname      | Delete |
| Data 1                              | 172.19.1.86/24 | buttercup.run |        |
| Data 2                              | 172.19.2.86/24 | buttercup.run |        |
| Management                          | 172.19.0.86/24 | buttercup.run |        |

Configuring IP Interfaces

The Management Appliance > Network > IP Interfaces page (and `interfaceconfig` command) enables you to add, edit, or delete IP interfaces.



Note

You cannot change the name or Ethernet port associated with the Management interface on the Security Management appliance. Further, the Security Management appliance does not support all of the features discussed below (Virtual Gateways, for example).

The following information is required when you configure an IP interface:

Table A-2      IP Interface Components

|                         |                                                                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                    | The nickname of the interface.                                                                                                                                                                   |
| IP address              | IP addresses within the same subnet cannot be configured on separate physical Ethernet interfaces.                                                                                               |
| Netmask (or subnetmask) | You can enter the netmask in standard dotted octet form (for example, 255.255.255.0) or hexadecimal form (for example, 0xfffff00). The default netmask is 255.255.255.0, a common class C value. |



**Table A-2** *IP Interface Components (continued)*

|                          |                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Broadcast address</b> | AsyncOS automatically calculates the default broadcast address from the IP address and the netmask.                                                                                                                                                                                                                                                               |
| <b>Hostname</b>          | The hostname that is related to the interface. This hostname is used to identify the server during the SMTP conversation. You are responsible for entering a valid hostname associated with each IP address. The software does not check that DNS correctly resolves the hostname to the matching IP address, or that reverse DNS resolves to the given hostname. |
| <b>Allowed services</b>  | FTP, SSH, Telnet, Cisco IronPort Spam Quarantine, HTTP, and HTTPS can be enabled or disabled on the interface. You can configure the port for each service. You can also specify the HTTP/HTTPS, port, and URL for the Cisco IronPort Spam Quarantine.                                                                                                            |



**Note**

If you have completed the System Setup Wizard as described in [Chapter 2, “Setup and Installation”](#) and committed the changes, one or two interfaces should already be configured on your appliance. (Refer to the settings you entered in the “Assign and Configure Logical IP Interface(s)” section.) In addition, the Management interface is configured on the Cisco IronPort appliance.

## Creating IP Interfaces Using the GUI

To create an IP interface:

1. Click **Add IP Interface** on the Management Appliance > Network > IP Interfaces page. The Add IP Interface page appears.

Figure A-2      Add IP Interface Page

**Add IP Interface**

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

Warnings - \* Please exercise care when disabling or changing these items, as this could disrupt active connections to this appliance when changes to these li  
\*\* Hyperlinks and URLs affected by these changes will not be usable until the changes are committed.

2. Enter a name for the interface.
3. Select an Ethernet port and enter an IP address.
4. Enter the netmask for the IP address.
5. Enter a hostname for the interface.
6. Select the check box next to each service you want to enable on this IP interface. Change the corresponding port if necessary.
7. Select whether to enable redirecting HTTP to HTTPS for appliance management on the interface.
8. If you are using the Cisco IronPort Spam Quarantine, you can select HTTP or HTTPS or both and specify the port numbers for each. You can also select whether to redirect HTTP requests to HTTPS. Finally, you can specify

whether the IP interface is the default interface for the Cisco IronPort Spam Quarantine, and whether to use the hostname as the URL or provide a custom URL.

9. Submit and commit your changes.

## FTP Access

To access the appliance via FTP, follow these steps:



### Warning

**By disabling services via the Management Appliance > Network > IP Interfaces page or the `interfaceconfig` command, you can disconnect yourself from the GUI or CLI, depending on how you are connected to the appliance. 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.**

1. Use the Management Appliance > Network > IP Interfaces page (or the `interfaceconfig` command) to enable FTP access for the interface.

In this example, the Management interface is edited to enable FTP access on port 21 (the default port):

**Figure A-3** *Edit IP Interface Page*

### 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:             | Service                                    | Port |
|                       | <input checked="" type="checkbox"/> FTP    | 21   |
|                       | <input checked="" type="checkbox"/> Telnet | 23   |
|                       | <input checked="" type="checkbox"/> SSH    | 22 * |



**Note** Remember to commit your changes before moving on to the next step.

- 2. Access the interface via FTP. Ensure you are using the correct IP address for the interface. Example:  
`ftp 192.168.42.42`  
  
Many browsers also allow you to access interfaces via FTP. Example:  
`ftp://192.10.10.10`
- 3. Browse to the directory for the specific task you are trying to accomplish. After you have accessed an interface via FTP, you can browse the following directories to copy and add (“GET” and “PUT”) files. See [Table A-3](#).

**Table A-3** Directories Available for Access

| Directory Name                                                                                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /avarchive<br>/bounces<br>/cli_logs<br>/delivery<br>/error_logs<br>/ftpd_logs<br>/gui_logs<br>/mail_logs<br>/rptd_logs<br>/sntpd.logs<br>/status<br>/system_logs | Created automatically for logging via the Management Appliance > System Administration > Log Subscriptions page or the <code>logconfig</code> and <code>rollovernow</code> commands. See the “Logging” chapter in the <i>Cisco IronPort AsyncOS for Email Advanced User Guide</i> for a detailed description of each log.<br><br>See “Log File Type Comparison” in the “Logging” chapter for the differences among each log file type. |

**Table A-3**      **Directories Available for Access (continued)**

| Directory Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /configuration | <p>The directory where data from the following pages and commands are exported to and/or imported (saved) from:</p> <ul style="list-style-type: none"> <li>• Virtual Gateway mappings (<code>altsrchost</code>)</li> <li>• Configuration data in XML format (<code>saveconfig</code>, <code>loadconfig</code>)</li> <li>• Host Access Table (HAT) page (<code>hostaccess</code>)</li> <li>• Recipient Access Table (RAT) page (<code>rcptaccess</code>)</li> <li>• SMTP Routes page (<code>smtproutes</code>)</li> <li>• Alias tables (<code>aliasconfig</code>)</li> <li>• Masquerading tables (<code>masquerade</code>)</li> <li>• Message filters (<code>filters</code>)</li> <li>• Global unsubscribe data (<code>unsubscribe</code>)</li> <li>• Test messages for the <code>trace</code> command</li> </ul> |

Table A-3      Directories Available for Access (continued)

| Directory Name    | Description                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /MFM              | The Mail Flow Monitoring database directory contains data for the Mail Flow Monitor functionality available from the GUI. Each subdirectory contains a README file that documents the record format for each file.                                         |
|                   | You can copy these files to a different machine for record keeping, or load the files into a database and create your own analysis application. The record format is the same for all files in all directories; this format may change in future releases. |
| /periodic_reports | The directory where all archived reports configured on the system are stored.                                                                                                                                                                              |

4. Use your FTP program to upload and download files to and from the appropriate directory.

## Secure Copy (scp) Access

If your client operating system supports a secure copy (scp) command, you can copy files to and from the directories listed in [Table A-3 on page A-6](#). For example, in the following example, the file `/tmp/test.txt` is copied from the client machine to the configuration directory of the appliance with the hostname `mail3.example.com`.



**Note**

The command prompts for the user's password (admin). This example is shown for reference only; your operating system's implementation of secure copy may vary.

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
```

The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.

DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of
known hosts.
```

```
admin@mail3.example.com's password: (type the password)
```

```
test.txt                100% | ***** | 1007
00:00
```

```
%
```

In this example, the same file is copied from the appliance to the client machine:

```
% scp admin@mail3.example.com:configuration/text.txt .
```

```
admin@mail3.example.com's password: (type the password)
```

```
test.txt                100% | ***** | 1007
00:00
```

You can use secure copy (`scp`) as an alternative to FTP to transfer files to and from the Cisco IronPort appliance.



#### Note

Only users in the operators and administrators group can use secure copy (`scp`) to access the appliance. For more information, see [Reverting to an Earlier Version of AsyncOS, page 12-25](#).

## Accessing via a Serial Connection

If you are connecting to the appliance via a serial connection, [Figure A-4](#) illustrates the pin numbers for the serial port connector, and [Table A-4](#) defines the pin assignments and interface signals for the serial port connector.

**Figure A-4      Pin Numbers for the Serial Port**

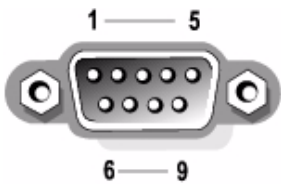


**Table A-4      Serial Port Pin Assignments**

| Pin   | Signal | I/O | Definition          |
|-------|--------|-----|---------------------|
| 1     | DCD    | I   | Data carrier detect |
| 2     | SIN    | I   | Serial input        |
| 3     | SOUT   | O   | Serial output       |
| 4     | DTR    | O   | Data terminal ready |
| 5     | GND    | n/a | Signal ground       |
| 6     | DSR    | I   | Data set ready      |
| 7     | RTS    | I   | Request to send     |
| 8     | CTS    | O   | Clear to send       |
| 9     | RI     | I   | Ring indicator      |
| Shell | n/a    | n/a | Chassis ground      |





## APPENDIX **B**

# Assigning Network and IP Addresses

---

This appendix describes general rules on networks and IP address assignments, and it presents some strategies for connecting the Cisco IronPort appliance to your network.

Topics included in this appendix include:

- [Ethernet Interfaces, page B-1](#)
- [Selecting IP Addresses and Netmasks, page B-2](#)
- [Strategies for Connecting Your Cisco IronPort Appliance, page B-4](#)

## Ethernet Interfaces

The Cisco IronPort X1050, C650, and C350 appliances are equipped with as many as four Ethernet interfaces located on the rear panel of the system, depending on the configuration (whether or not you have the optional optical network interface). They are labeled:

- Management
- Data1
- Data2
- Data3
- Data4

# Selecting IP Addresses and Netmasks

When you configure the network, the Cisco IronPort appliance must be able to select a unique interface to send an outgoing packet. This requirement drives some of the decisions regarding IP address and netmask selection for the Ethernet interfaces. The rule is that only one interface can be on a single network (as determined through the applications of netmasks to the IP addresses of the interfaces).

An IP address identifies a physical interface on any given network. A physical Ethernet interface can have more than one IP address for which it accepts packets. An Ethernet interface that has more than one IP address can send packets over that interface with any one of the IP addresses as the source address in the packet. This property is used in implementing Virtual Gateway technology.

The purpose of a netmask is to divide an IP address into a network address and a host address. The network address can be thought of as the network part (the bits matching the netmask) of the IP address. The host address is the remaining bits of the IP address. The number of bits in a four octet address that are significant are sometimes expressed in Classless Inter-Domain Routing (CIDR) style. This is a slash followed by the number of bits (1-32).

A netmask can be expressed in this way by simply counting the ones in binary, so 255.255.255.0 becomes “/24” and 255.255.240.0 becomes “/20.”

## Sample Interface Configurations

This section shows sample interface configurations based on some typical networks. The example uses two interfaces called Int1 and Int2. In the case of the Cisco IronPort appliance, these interface names can represent any two interfaces out of the three Cisco IronPort interfaces (Management, Data1, Data2).

### Network 1:

Separate interfaces must appear to be on separate networks.

| Interface | IP Address   | Netmask       | Net Address    |
|-----------|--------------|---------------|----------------|
| Int1      | 192.168.1.10 | 255.255.255.0 | 192.168.1.0/24 |
| Int2      | 192.168.0.10 | 255.255.255.0 | 192.168.0.0/24 |

Data addressed to 192.168.1.x (where X is any number from 1 through 255, except for your own address, 10 in this case) go out on Int1. Anything addressed to 192.168.0.x goes out on Int2. Any packet headed for some other address not in these formats, most likely out on a WAN or the Internet, is sent to the default gateway, which must be on one of these networks. The default gateway then forwards the packet on.

### Network 2:

The network addresses (network parts of the IP addresses) of two different interfaces cannot be the same.

| Ethernet Interface | IP Address   | Netmask     | Net Address    |
|--------------------|--------------|-------------|----------------|
| Int1               | 192.168.1.10 | 255.255.0.0 | 192.168.0.0/16 |
| Int2               | 192.168.0.10 | 255.255.0.0 | 192.168.0.0/16 |

This situation presents a conflict in that two different Ethernet interfaces have the same network address. If a packet from the Cisco IronPort appliance is sent to 192.168.1.11, there is no way to decide which Ethernet interface should be used to deliver the packet. If the two Ethernet interfaces are connected to two separate physical networks, the packet may be delivered to the incorrect network and never find its destination. The Cisco IronPort appliance does not allow you to configure your network with conflicts.

You can connect two Ethernet interfaces to the same physical network, but you must construct IP addresses and netmasks to allow the Cisco IronPort appliance to select a unique delivery interface.

## IP Addresses, Interfaces, and Routing

When you select an interface on which to perform a command or function in the GUI or CLI that allows you to select an interface (for example, upgrading AsyncOS or configuring DNS), routing (your default gateway) takes precedence over your selection.

For example, suppose that you have an Cisco IronPort appliance with the three network interfaces configured, each on a different network segment (assume all /24):

| <b>Ethernet</b>   | <b>IP</b>    |
|-------------------|--------------|
| <b>Management</b> | 192.19.0.100 |
| <b>Data1</b>      | 192.19.1.100 |
| <b>Data2</b>      | 192.19.2.100 |

And your default gateway is 192.19.0.1.

Now, if you perform an AsyncOS upgrade (or other command or function that allows you to select an interface) and you select the IP that is on Data1 (192.19.1.100), you would expect all the TCP traffic to occur over the Data1 Ethernet interface. However, instead the traffic goes out of the interface that is set as your default gateway, in this case Management, but is stamped with the source address of the IP on Data1.

## Summary

The Cisco IronPort appliance must always be able to identify a unique interface over which a packet can be delivered. To make this decision, the Cisco IronPort appliance uses a combination of the packet's destination IP address, and the network and IP address settings of its Ethernet interfaces. The following table summarizes the preceding examples:

|                                     | <b>Same Network</b> | <b>Different Network</b> |
|-------------------------------------|---------------------|--------------------------|
| <b>Same Physical Interface</b>      | Allowed             | Allowed                  |
| <b>Different Physical Interface</b> | Not allowed         | Allowed                  |

## Strategies for Connecting Your Cisco IronPort Appliance

Keep the following in mind when connecting your Cisco IronPort appliance:

- Administrative traffic (CLI, web interface, log delivery) is usually little compared to email traffic.
- If two Ethernet interfaces are connected to the same network switch, but end up talking to a single interface on another host downstream, or are connected to a network hub where all data are echoed to all ports, no advantage is gained by using two interfaces.
- SMTP conversations over an interface operating at 1000Base-T are slightly faster than conversations over the same interfaces operating at 100Base-T, but only under ideal conditions.
- There is no point in optimizing connections to your network if there is a bottleneck in some other part of your delivery network. Bottlenecks most often occur in the connection to the Internet and further upstream at your connectivity provider.

The number of Cisco IronPort appliance interfaces that you choose to connect and how you address them should be dictated by the complexity of your underlying network. It is not necessary to connect multiple interfaces if your network topology or data volumes do not call for it. It is also possible to keep the connection simple at first as you familiarize yourself with the gateway and then increase the connectivity as volume and network topology require it.





# APPENDIX C

## Firewall Information

---

The following table lists the possible ports that may need to be opened for proper operation of the Cisco IronPort appliance (these are the default values).

**Table C-1**      **Firewall Ports**

| Port  | Protocol | In/Out    | Hostname                | Description                                                                |
|-------|----------|-----------|-------------------------|----------------------------------------------------------------------------|
| 20/21 | TCP      | In or out | AsyncOS IPs, FTP server | FTP for aggregation of log files.                                          |
| 22    | SSH      | Out       | AsyncOS IPs             | Centralized configuration manager configuration push.                      |
| 22    | TCP      | In        | AsyncOS IPs             | SSH access to the CLI, aggregation of log files.                           |
| 22    | TCP      | Out       | SCP server              | SCP push to log server.                                                    |
| 23    | Telnet   | In        | AsyncOS IPs             | Telnet access to the CLI.                                                  |
| 23    | Telnet   | Out       | Telnet server           | Telnet upgrades.                                                           |
| 25    | TCP      | Out       | Any                     | SMTP to send email.                                                        |
| 25    | TCP      | In        | AsyncOS IPs             | SMTP to receive bounced email or if injecting email from outside firewall. |
| 80    | HTTP     | In        | AsyncOS IPs             | HTTP access to the GUI for system monitoring.                              |
| 80    | HTTP     | Out       | downloads.cisco.com     | Service updates, except for AsyncOS upgrades.                              |
| 80    | HTTP     | Out       | updates.cisco.com       | AsyncOS upgrades.                                                          |

**Table C-1 Firewall Ports (continued)**

|             |         |     |                          |                                                                                                                        |
|-------------|---------|-----|--------------------------|------------------------------------------------------------------------------------------------------------------------|
| 82          | HTTP    | In  | AsyncOS IPs              | Used for viewing the Cisco IronPort Spam Quarantine.                                                                   |
| 83          | HTTPS   | In  | AsyncOS IPs              | Used for viewing the Cisco IronPort Spam Quarantine.                                                                   |
| 53          | UDP/TCP | Out | DNS servers              | DNS if configured to use Internet root servers or other DNS servers outside the firewall. Also for SenderBase queries. |
| 110         | TCP     | Out | POP server               | POP authentication for end users for Cisco IronPort Spam Quarantine.                                                   |
| 123         | UDP     | Out | NTP server               | NTP if time servers are outside firewall.                                                                              |
| 143         | TCP     | Out | IMAP server              | IMAP authentication for end users for Cisco IronPort Spam Quarantine.                                                  |
| 161         | UDP     | In  | AsyncOS IPs              | SNMP queries.                                                                                                          |
| 162         | UDP     | Out | Management station       | SNMP traps.                                                                                                            |
| 389<br>3268 | LDAP    | Out | LDAP servers             | LDAP if LDAP directory servers are outside firewall. LDAP authentication for Cisco IronPort Spam Quarantine.           |
| 636<br>3269 | LDAPS   | Out | LDAPS                    | LDAPS — ActiveDirectory's global catalog server.                                                                       |
| 443         | TCP     | In  | AsyncOS IPs              | Secure HTTP ( <a href="https">https</a> ) access to the GUI for system monitoring.                                     |
| 443         | TCP     | Out | update-static.cisco.com  | Verify the latest files for the update server.                                                                         |
| 443         | TCP     | Out | phonehome.senderbase.org | Receive/send Outbreak Filters.                                                                                         |
| 514         | UDP/TCP | Out | Syslog server            | Syslog logging.                                                                                                        |



**Table C-1**      **Firewall Ports (continued)**

|      |     |            |             |                                                                                                                                          |
|------|-----|------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 2222 | CCS | In and out | AsyncOS IPs | Cluster Communication Service (for centralized management).                                                                              |
| 6025 | TCP | In         | AsyncOS IPs | Send Cisco IronPort Spam Quarantine data to the Security Management appliance if the external Cisco IronPort Spam Quarantine is enabled. |





# APPENDIX **D**

## Examples

---

This appendix illustrates and describes a number of common ways to implement the Security Management appliance, and includes the following sections:

- [Example 1: Investigating a User, page D-2](#)
- [Example 2: Tracking a URL, page D-7](#)
- [Example 3: Investigating Top URL Categories Visited, page D-8](#)
- [Example 4: Privacy and Hiding User Names, page D-12](#)
- [Example 5: Upgrading to a New Configuration Master on an Existing Security Management Appliance, page D-15](#)
- [Example 6: Importing a Configuration File from an Existing Web Security Appliance, page D-17](#)
- [Example 7: Customizing Access Policies on Remote Web Security Appliances and Managing Them on a Central Security Management Appliance, page D-20](#)

## Web Security Appliance Examples

This section describes examples using a Security Management appliance and Web Security appliances.

**Note**

All of these scenario assumes that you have enabled web reporting and web tracking on the Security Management appliance *and* on your Web Security appliances. For information on how to enable web tracking and web reporting, see [Enabling and Disabling Centralized Web Reporting on a Security Management Appliance](#).

## Example 1: Investigating a User

This example demonstrates how a system administrator would investigate a particular user at a company.

In this scenario, a manager has gotten a complaint that an employee is visiting inappropriate web sites at work. To investigate this, the system administrator now needs to track the details of their web activity.

Once the web activity is tracked, a web report is generated with information about the employee's browsing history.

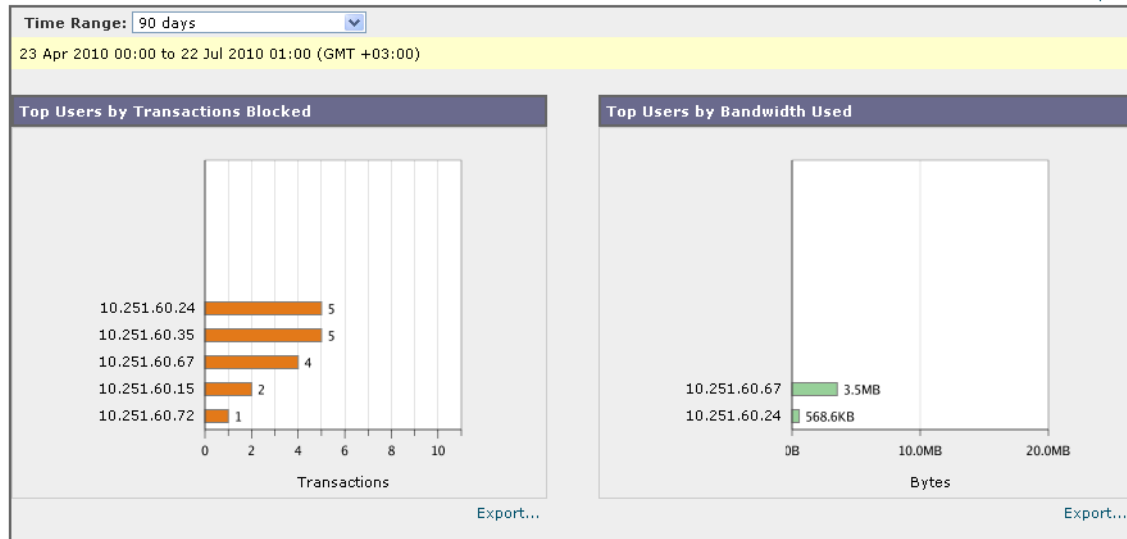
---

**Step 1** On the Security Management appliance, choose **Web > Reporting > Users**.  
The Users page appears.

**Step 2** In the Users table, click on the **User ID** or **Client IP address** you want to investigate.

If you do not know the User ID or the Client IP address, type what you can remember of the User ID or Client IP address in text field, and click on **Find User ID or Client IP address**. The IP address does not need to be an exact match to return results. The Users table is populated with the User ID and Client IP addresses that you have specified. In this example, we are looking for information on Client IP address 10.251.60.24.

## Users

[Printable \(PDF\)](#)

**Step 3** Click on IP address **10.251.60.24**.

The User Details page appears for 10.251.60.24.

Users > 10.251.60.24

[Printable \(PDF\)](#)

Time Range: 90 days

23 Apr 2010 00:00 to 22 Jul 2010 01:42 (GMT +03:00)

URL Categories by Total Transactions

| URL Category               | Transactions |
|----------------------------|--------------|
| Search Engines and Portals | 99           |
| Business and Industry      | 7            |
| Computers and Internet     | 5            |
| Advertisements             | 4            |
| Infrastructure             | 3            |

Trend by Total Transactions

| Date   | Transactions |
|--------|--------------|
| 25-Apr | 0            |
| 09-May | 0            |
| 23-May | 0            |
| 06-Jun | 0            |
| 20-Jun | 0            |
| 04-Jul | 0            |
| 18-Jul | 118          |

Export...

URL Categories Matched

| URL Category                 | Bandwidth Used | Time Spent | Blocked URL Category | Transactions Completed | Total Transactions |
|------------------------------|----------------|------------|----------------------|------------------------|--------------------|
| Search Engines and Portals   | 447.4KB        | 00:21      | 0                    | 99                     | 99                 |
| Business and Industry        | 15.5KB         | 00:06      | 0                    | 7                      | 7                  |
| Computers and Internet       | 84.4KB         | 00:06      | 0                    | 5                      | 5                  |
| Advertisements               | 16.9KB         | 00:00      | 0                    | 4                      | 4                  |
| Infrastructure               | 4,540B         | 00:00      | 0                    | 3                      | 3                  |
| Totals (all available data): | 568.6KB        | 00:33      | 0                    | 118                    | 118                |

Find URL Category

Columns... | Export...

Domains Matched

Data below is not available for the full time range selected. Data for this table is available for 13 Jul 2010 01:00 to 14 Jul 2010 23:59 (GMT +03:00). Click to change the time range of this report to reflect the data available.

Change Time Range

| Domain or IP         | Bandwidth Used | Time Spent | Transactions Completed | Transactions Blocked | Total Transactions |
|----------------------|----------------|------------|------------------------|----------------------|--------------------|
| google.com           | 464.5KB        | 00:36      | 101                    | 5                    | 106                |
| gmodules.com         | 83.1KB         | 00:06      | 4                      | 0                    | 4                  |
| google-analytics.com | 8,272B         | 00:00      | 4                      | 0                    | 4                  |
| doubleclick.net      | 15.1KB         | 00:00      | 3                      | 0                    | 3                  |
| kontera.com          | 6,391B         | 00:06      | 2                      | 0                    | 2                  |
| addthis.com          | 1,365B         | 00:00      | 1                      | 0                    | 1                  |
| addthiscdn.com       | 1,231B         | 00:00      | 1                      | 0                    | 1                  |
| quantserve.com       | 1,847B         | 00:00      | 1                      | 0                    | 1                  |
| yandex.ru            | 2,021B         | 00:00      | 1                      | 0                    | 1                  |

Find Domain or IP

Columns... | Export...

Applications Matched

No data was found in the selected time range

Malware Threats Detected

No data was found in the selected time range

Policies Matched

| Policy Name                  | Policy Type | Bandwidth Used | Completed Transactions | Blocked Transactions | Total Transactions |
|------------------------------|-------------|----------------|------------------------|----------------------|--------------------|
| DefaultGroup                 | Access      | 568.6KB        | 118                    | 0                    | 118                |
| NONE                         | Access      | 0B             | 0                      | 5                    | 5                  |
| Totals (all available data): | --          | 568.6KB        | 118                    | 5                    | 123                |

From the User Details page you can determine the URL Categories by Total Transactions, Trend by Total Transaction, URL Categories Matched, Domains Matched, Applications Matched, Malware Threats Detected, and Policies Matched.

These categories allow you to find out if, for example, user 10.251.60.24 was trying to access blocked URLs, which could be viewed in the Transactions Blocked column under the Domains section on the page.

- Step 4** Click **Export** under the Domains Matched table to view the entire list of Domains and URLs that the user tried to access.

Figure D-1 shows you an exported list of information that has been exported from the user.

**Figure D-1 Sample Export Data**

|    | A                    | B              | C          | D                          | E                      | F                    | G                  |
|----|----------------------|----------------|------------|----------------------------|------------------------|----------------------|--------------------|
|    | Domain or IP         | Bandwidth Used | Time Spent | Other Blocked Transactions | Transactions Completed | Transactions Blocked | Total Transactions |
| 1  | addthis.com          | 1365           | 0          | 0                          | 1                      | 0                    | 1                  |
| 2  | addthiscdn.com       | 1231           | 0          | 0                          | 1                      | 0                    | 1                  |
| 3  | doubleclick.net      | 15447          | 0          | 0                          | 3                      | 0                    | 3                  |
| 4  | gmodules.com         | 85071          | 360        | 0                          | 4                      | 0                    | 4                  |
| 5  | google-analytics.com | 8272           | 0          | 0                          | 4                      | 0                    | 4                  |
| 6  | google.com           | 475631         | 2160       | 5                          | 101                    | 5                    | 106                |
| 7  | kontera.com          | 6391           | 360        | 0                          | 2                      | 0                    | 2                  |
| 8  | quantserve.com       | 1847           | 0          | 0                          | 1                      | 0                    | 1                  |
| 9  | yandex.ru            | 2021           | 0          | 0                          | 1                      | 0                    | 1                  |
| 10 |                      |                |            |                            |                        |                      |                    |
| 11 |                      |                |            |                            |                        |                      |                    |
| 12 |                      |                |            |                            |                        |                      |                    |

From here you can use the Web Tracking feature to track and view this specific user's web usage.



#### Note

It is important to remember that web reporting allows you to retrieve all the domain information that a user goes to, not necessarily the specific URL that is accessed. For information on a specific URL that the user is accessing, what time they went to that URL, whether that URL is allowed, etc., use the Web Tracking page.

- Step 5** Choose **Web > Reporting > Web Tracking**.

- Step 6** In the User/Client IP Address text field type in the user name or IP address.

In this example we are searching for web tracking information for user 10.251.60.24.

The Web Tracking page appears.

Web Tracking

Search

Available: 13 Jul 2010 01:00 to 14 Jul 2010 23:59 (GMT +03:00)

Time Range:

90 days

User/Client IP:

10.251.60.24

(e.g. jdoe or DOMAIN(jdoe))

Website:

(e.g. google.com)

Transaction Type:

All Transactions

Advanced

Search transactions using advanced criteria.

Clear

Search

Results

Displaying 1 - 8 of 8 transactions.

| Time (GMT +03:00)    | Transaction                                                             | Display Details... | Disposition | Bandwidth | User / Client IP |
|----------------------|-------------------------------------------------------------------------|--------------------|-------------|-----------|------------------|
| 14 Jul 2010 22:58:32 | http://safebrowsing.clients.google.com/safebrowsing/downloads?cli...    |                    | Allow       | 6,354B    | 10.251.60.24     |
| 14 Jul 2010 22:27:37 | http://safebrowsing.clients.google.com/safebrowsing/downloads?cli...    |                    | Allow       | 5,131B    | 10.251.60.24     |
| 14 Jul 2010 21:56:02 | http://safebrowsing.clients.google.com/safebrowsing/downloads?cli...    |                    | Allow       | 8,148B    | 10.251.60.24     |
| 14 Jul 2010 21:28:05 | http://kona5.kontera.com/KonaGet.js?u=1279132089362&p=142924&...        |                    | Allow       | 6,391B    | 10.251.60.24     |
| 14 Jul 2010 21:27:49 | http://k830suiki828goudg9448o6bp0tpu5r3.a.friendconnect.gmodules....    |                    | Allow       | 83.1KB    | 10.251.60.24     |
| 14 Jul 2010 21:27:44 | http://www.google.com/url?sa=t&source=web&cd=1&ved=0C...                |                    | Allow       | 244.3KB   | 10.251.60.24     |
| 14 Jul 2010 21:27:04 | http://www.google.com/search?q=%D0%BF%D0%BE%D0%BB%D1%8C...%D0%BA%D0%... |                    | Allow       | 28.4KB    | 10.251.60.24     |
| 14 Jul 2010 21:26:58 | http://suggestqueries.google.com/complete/search?output=firefox&a...    |                    | Block       | 14.6KB    | 10.251.60.24     |

Displaying 1 - 8 of 8 transactions.

Columns...

From this page you can view a full list of transactions and URLs that the user 10.251.60.24 has visited.

Related Topics

Table D-1 lists each of the topics discussed in this example. Click on the link for details on each topic.

Table D-1 Related Topics for Investigating a User

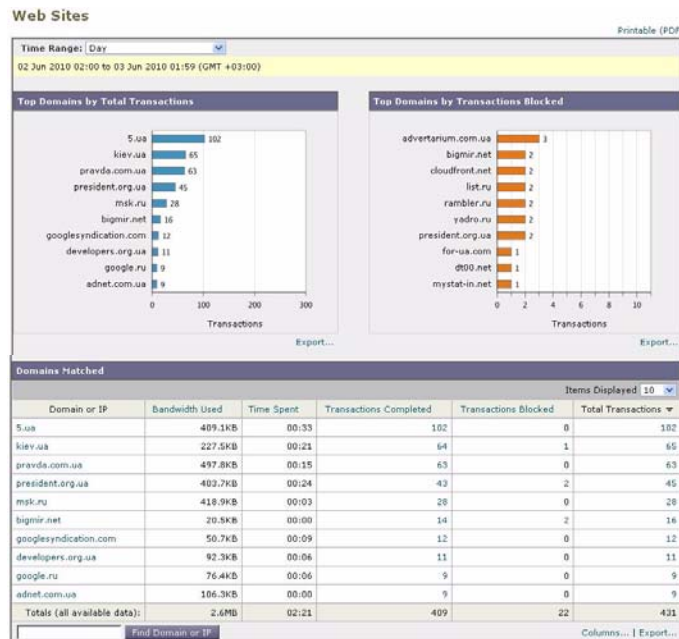
| Feature Name          | Feature Information                                           |
|-----------------------|---------------------------------------------------------------|
| User Page             | <a href="#">Users Page, page 5-16</a>                         |
| User Details Page     | <a href="#">User Details Page, page 5-20</a>                  |
| Exporting Report Data | <a href="#">Printing and Exporting Report Data, page 3-20</a> |
| Web Tracking          | <a href="#">Web Tracking Page, page 5-69</a>                  |



## Example 2: Tracking a URL

In this scenario, a Sales manager wants to find out what the top five visited web sites are at their company are for the last week. Additionally, the manager wants to know which users are going to those websites.

- Step 1** On the Security Management appliance, choose **Web > Reporting > Web Sites**. The Web Sites page appears.



- Step 2** From the Time Range drop-down list, choose **Week**.

- Step 3** Scroll down to the Domains section to view the domains, or web sites that have been visited.

The top 25 web sites that have been visited will be displayed in the Domains Matched table. In the same table you can click on the link in the Domain or IP column to view the actual web sites for a particular address or user.

## Related Topics

[Table D-2](#) lists each of the topics discussed in this example. Click on the link for details on each topic.

**Table D-2**      *Related Topics for Tracking a URL*

| Feature Name   | Feature Information                       |
|----------------|-------------------------------------------|
| Web Sites Page | <a href="#">Web Sites Page, page 5-24</a> |

## Example 3: Investigating Top URL Categories Visited

In this scenario, the Human Resources manager wants to know what the top three URL categories her employees are visiting over the 30 days. Additionally, a network manager wants to get this information to monitor bandwidth usage, to find out what URLs are taking up the most bandwidth on her network.

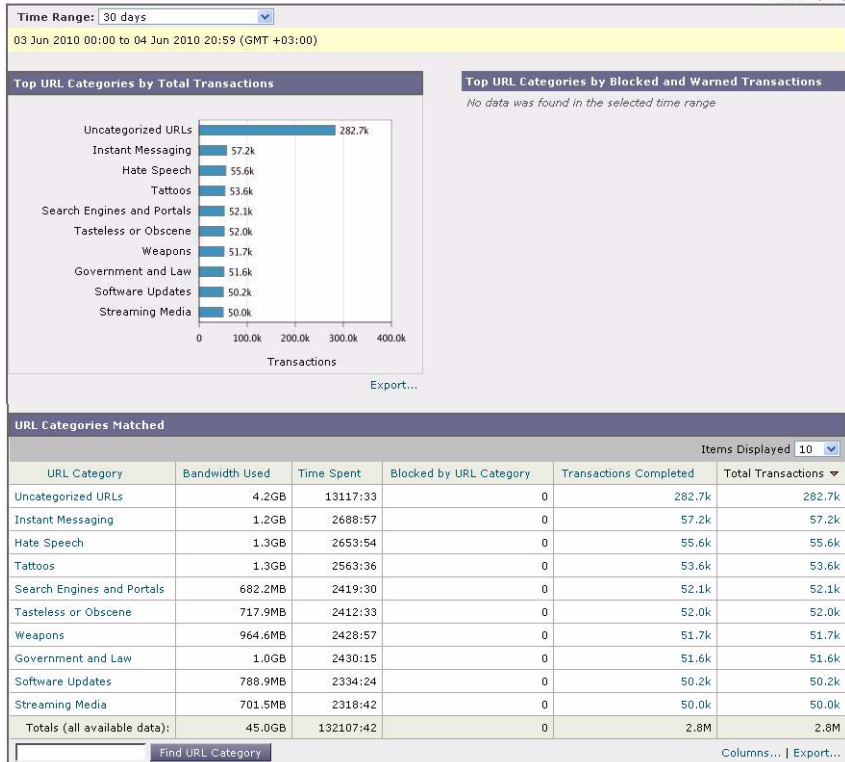
The example below is to show how you can gather data for several people covering several points of interest, while only having to generate one report.

**Step 1**      On the Security Management appliance, choose **Web > Reporting > URL Categories**.

The URL Categories page appears.

## URL Categories

Printable (PDF)



From the URL Categories page in this example, you can see that of the top 10 URL Categories by Total Transactions graph reveals, there were 282 K of Uncategorized URLs that were accessed, as well as Instant Messaging, Hate Speech and Tattoo sites, and so forth.

At this point you can export that raw data to an Excel spreadsheet, by clicking the **Export** link and send this file to the Human Resources manager. But remember, your network manager wants to know the bandwidth usage by each URL.

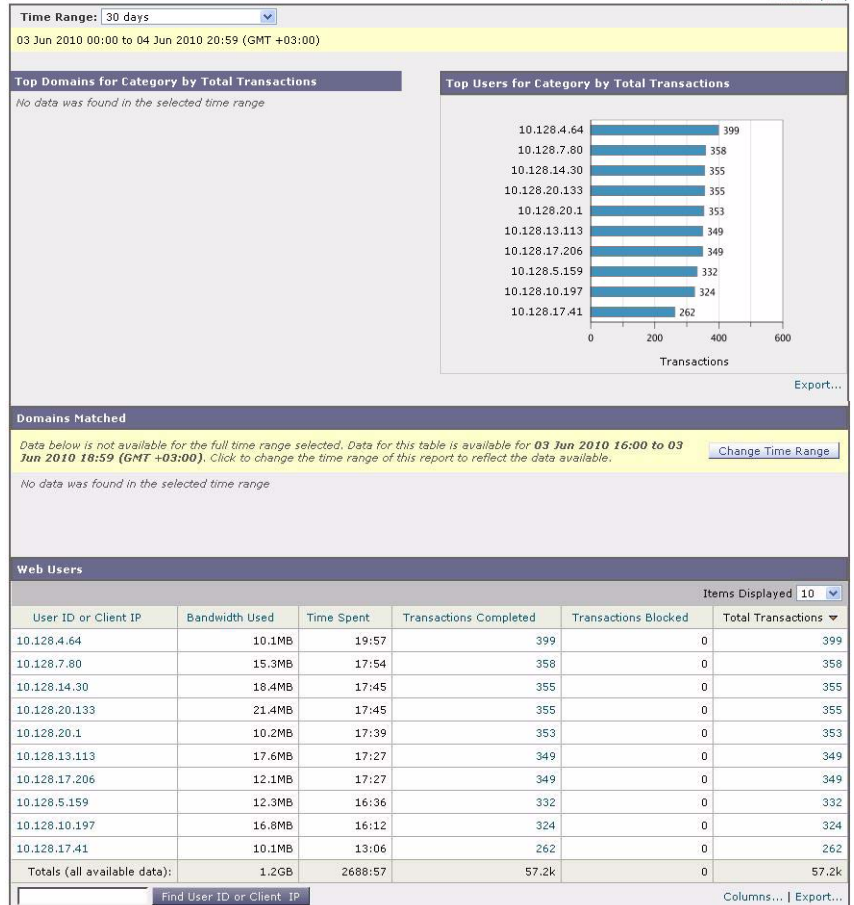
**Step 2** Scroll down to the **URL Categories Matched** table, to view the Bandwidth Used column.

| URL Categories Matched                   |                |            |                         |                        |                      |
|------------------------------------------|----------------|------------|-------------------------|------------------------|----------------------|
|                                          |                |            |                         |                        | Items Displayed 10 ▾ |
| URL Category                             | Bandwidth Used | Time Spent | Blocked by URL Category | Transactions Completed | Total Transactions ▾ |
| Uncategorized URLs                       | 4.2GB          | 13117:33   | 0                       | 282.7k                 | 282.7k               |
| Instant Messaging                        | 1.2GB          | 2688:57    | 0                       | 57.2k                  | 57.2k                |
| Hate Speech                              | 1.3GB          | 2653:54    | 0                       | 55.6k                  | 55.6k                |
| Tattoos                                  | 1.3GB          | 2563:36    | 0                       | 53.6k                  | 53.6k                |
| Search Engines and Portals               | 682.2MB        | 2419:30    | 0                       | 52.1k                  | 52.1k                |
| Tasteless or Obscene                     | 717.9MB        | 2412:33    | 0                       | 52.0k                  | 52.0k                |
| Weapons                                  | 964.6MB        | 2428:57    | 0                       | 51.7k                  | 51.7k                |
| Government and Law                       | 1.0GB          | 2430:15    | 0                       | 51.6k                  | 51.6k                |
| Software Updates                         | 788.9MB        | 2334:24    | 0                       | 50.2k                  | 50.2k                |
| Streaming Media                          | 701.5MB        | 2318:42    | 0                       | 50.0k                  | 50.0k                |
| Totals (all available data):             | 45.0GB         | 132107:42  | 0                       | 2.8M                   | 2.8M                 |
| Find URL Category Columns...   Export... |                |            |                         |                        |                      |

From the **URL Categories Matched** table, you can see the Bandwidth Usage for all of the URL Categories. Again, you can click the **Export** link and send this file to the Network manager. For finer granularity though, click on the Instant Messaging link to find out which users are taking up the bandwidth. The following page appears.

## URL Categories &gt; Instant Messaging

Printable (PDF)



From this page, the network manager can see the top 10 users for Instant Messaging sites.

This pages reveals that in the last 30 days, user 10.128.4.64 has spent 19 hours and 57 minutes on an Instant Messaging site; and the bandwidth usage for this time was 10.1 MB.

## Related Topics

[Table D-3](#) lists each of the topics discussed in this example. Click on the link for details on each topic.

**Table D-3**      *Related Topics for Investigating the Top URL Categories*

| Feature Name          | Feature Information                                           |
|-----------------------|---------------------------------------------------------------|
| URL Categories Page   | <a href="#">URL Categories Page, page 5-28</a>                |
| Exporting Report Data | <a href="#">Printing and Exporting Report Data, page 3-20</a> |

## Example 4: Privacy and Hiding User Names

In this example, a manager wants to generate a set of reports, but does not want any personal information of his employees to be shown.

The Security Management appliance handles this by allowing you to enable or disable this action by clicking on the ‘Anonymize User Names in Reports’ checkbox. Once this is enabled, you can generate and distribute a report without revealing the usernames to the people receiving the reports.

The following example shows you what you can see on a report that shows personal information, such as User name or IP address, and what a report looks like after you have anonymized the user names.

### Before Enabling Anonymized User Names

- Step 1

On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.

The Centralized Web Reporting page appears.



**Note**

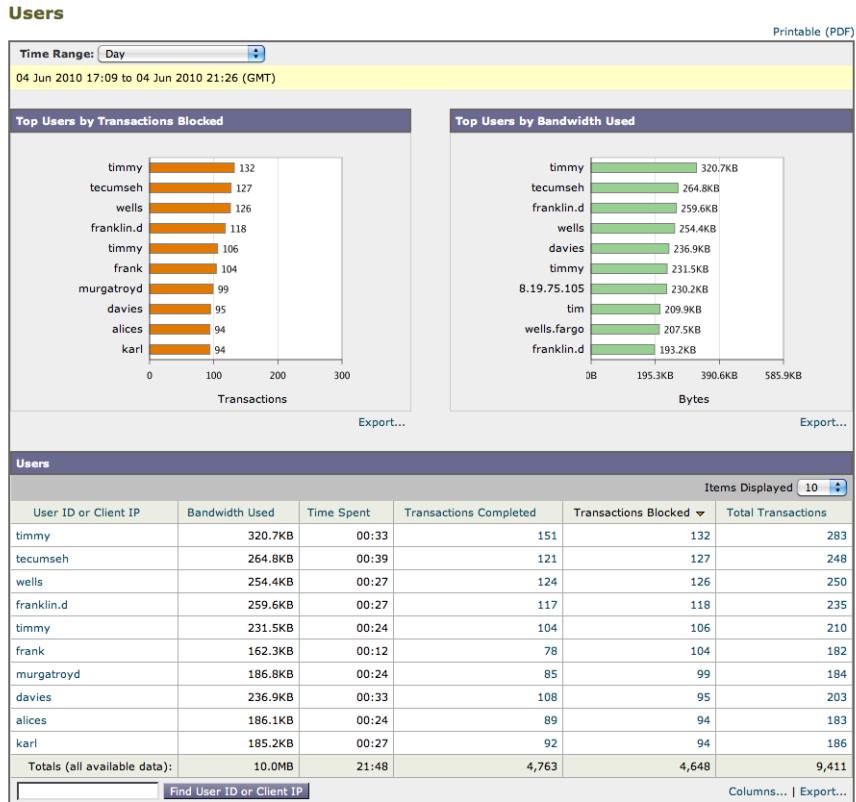
If you are enabling centralized reporting for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**. See the ‘[Configuring Centralized Web Reporting](#)’ section on page 5-3.

- Step 2

Click **Edit Settings**.
- Step 3

Make sure that the **Anonymize User Names in Reports** checkbox is unchecked.

- Step 4** Click **Submit**.
- Step 5** Choose **Web > Users**.
- Step 6** The Web Users page appears.



In this case, all user names *are* displayed on the **Web > Users** page.

The user name information is fine to show if you are the intended viewer of this information. But, if you do not want this information revealed to another group, you need to hide the user names.



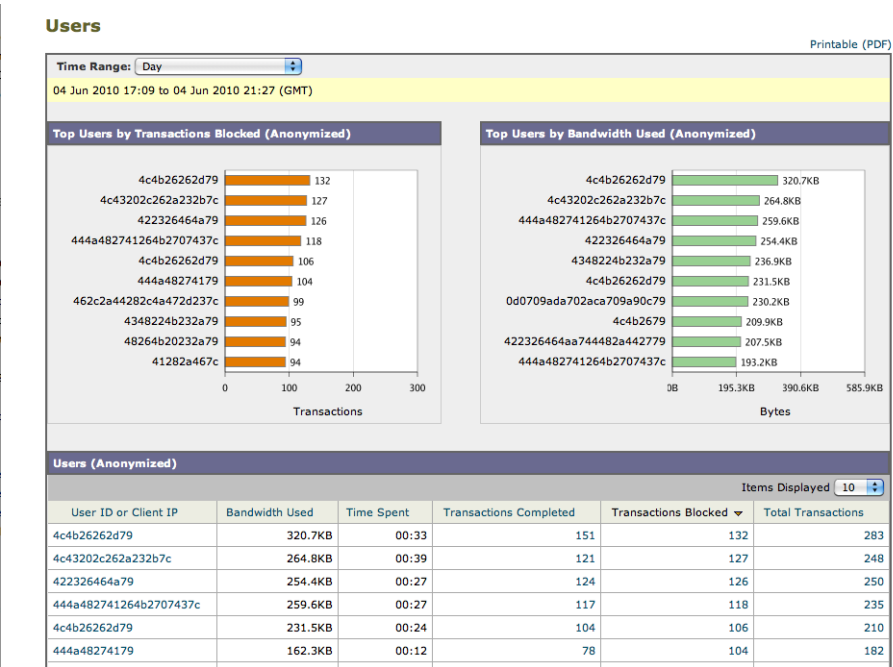
#### Note

If you have administrator status, you will always see the user names.

After Enabling the Anonymize Usernames in Reports

Here is what the same report looks like using the Anonymize User Names in Reports feature.

- Step 1
- On the Security Management appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.
- Step 2
- Click **Edit Settings**.
- Step 3
- Check the **Anonymize User Names in Reports** checkbox.
- Step 4
- Click **Submit**.
- Step 5
- Choose **Web > Users**.
- Step 6
- The Web Users page appears.



In this case, the user names are *not* displayed on the **Web > Users** page.



## Related Topics

Table D-4 lists each of the topics discussed in this example. Click on the link for details on each topic.

**Table D-4**      *Related Topics for Privacy Information*

| Feature Name           | Feature Information                                                         |
|------------------------|-----------------------------------------------------------------------------|
| Web Reporting          | <a href="#">`Getting Started with Web Reporting' section on page 5-3</a>    |
| Enabling Web Reporting | <a href="#">`Configuring Centralized Web Reporting' section on page 5-3</a> |
| User Page              | <a href="#">Users Page, page 5-16</a>                                       |

## Example 5: Upgrading to a New Configuration Master on an Existing Security Management Appliance



### Note

This example assumes that you have Configuration 6.3 initialized.

This example explains how to upgrade your existing Security Management appliance to a new configuration master.

In this example, the user has an existing Security Management appliance that is running Configuration Master 6.3, and wants to upgrade to Configuration Master 7.1.

To upgrade, perform the following steps:

- Step 1

On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

The Configuration Masters page appears.

Configuration Masters

| Configuration Masters                             |                         |                      |
|---------------------------------------------------|-------------------------|----------------------|
| Configuration Master Version                      | Assigned Web Appliances | Options              |
| 5.7 (5.7.1)                                       | 0 of 0                  | Initialize           |
| 6.3 (6.3.3)                                       | 0 of 0                  | Import Configuration |
| 7.1 (7.1.0)                                       | 0 of 0                  | Initialize           |
| <a href="#">Edit Appliance Assignment List...</a> |                         |                      |

From this page you can see that Configuration Master 6.3 has already been initialized, and Configuration Master 7.1 has not been initialized. This can also be verified by the fact that only one Configuration Master, Configuration Master 6.3, is shown under the Security Management appliance tabs.

**Step 2** In the 7.1 row, click **Initialize**.

Management ApplianceEmailWeb

ReportingUtilitiesConfiguration Master 6.3

No Changes Pending

**Initialize Configuration Master 7.1**

Initialization Options

Initial Settings:

☐ Copy configuration master: 6.3

☒ Copy custom roles

☐ Use default settings

Cancel

Initialize

- Step 3** Click the **Copy Configuration Master 6.3** radio button, and check the **Copy custom rules** checkbox.
- By checking the **Copying the custom rules** checkbox, you can maintain any user roles or specific policies that you currently have with the Configuration Master 6.3, and transfer that data to the new 7.1 Configuration Master.
- Step 4** Click **Initialize**.
- Configuration Master 7.1 is now initialized and ready for use.

# Related Topics

Table D-5 lists each of the topics discussed in this example. Click on the link for details on each topic.

**Table D-5**      *Related Topics for Upgrading a New Configuration Master*

| Feature Name          | Feature Information                                                      |
|-----------------------|--------------------------------------------------------------------------|
| Configuration Masters | <a href="#">`Working with Configuration Masters' section on page 8-3</a> |

# Example 6: Importing a Configuration File from an Existing Web Security Appliance



## Note

This example assumes that you have Configuration 6.3 initialized.

This example explains how to import an existing configuration file from a Web Security appliance into your existing Security Management appliance.

In this scenario, the user has decided to use centralized configuration management for all of their Web Security appliances. To do this, they have recently purchased a Security Management appliance to manage all of their Web Security appliances.

- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Centralized Configuration Manager**.
- Step 2** Click **Enable**.
- Step 3** Click on **Web > Utilities > Configuration Masters**.  
The Configuration Masters page appears.

## Configuration Masters

| Configuration Masters        |                         |                                                   |
|------------------------------|-------------------------|---------------------------------------------------|
| Configuration Master Version | Assigned Web Appliances | Options                                           |
| 5.7 (5.7.1)                  | 0 of 0                  | Initialize                                        |
| 6.3 (6.3.3)                  | 0 of 0                  | Import Configuration                              |
| 7.1 (7.1.0)                  | 0 of 0                  | Initialize                                        |
|                              |                         | <a href="#">Edit Appliance Assignment List...</a> |

From this page you can see that Configuration Master 6.3 has already been initialized, and Configuration Master 7.1 has not been initialized. This can also be verified by the fact that only one Configuration Master, Configuration Master 6.3, is shown under the Security Management appliance tabs.

**Step 4** In the 7.1 row, click **Initialize**.

Management Appliance | Email | **Web**

Reporting | Utilities | Configuration Master 6.3

No Changes Pending

### Initialize Configuration Master 7.1

Initialization Options

Initial Settings: ☒ Copy configuration master: 6.3  
☒ Copy custom roles  
☐ Use default settings

Cancel Initialize

**Step 5** Click the **Use Default Settings** radio button.

The Configuration Masters page is displayed with information that the initialization was successful.

Management Appliance | Email | **Web**

Reporting | Utilities | Configuration Master 7.1

Commit Changes

### Configuration Masters

Success — Configuration Master 7.1 was successfully initialized.

| Configuration Master Version | Assigned Web Appliances | Options              |
|------------------------------|-------------------------|----------------------|
| 5.7 (5.7.1)                  | 0 of 0                  | Initialize           |
| 6.3 (6.3.3)                  | 0 of 0                  | Initialize           |
| 7.1 (7.1.0)                  | 0 of 0                  | Import Configuration |

Edit Appliance Assignment List...

**Step 6** Click **Import Configuration**.

The Import Web Configuration page is displayed.

**Step 7** From the **Select Configuration Source** drop-down menu, choose **Web Configuration File**.

- Step 8** In the text field next to **Load a Valid Configuration File from a Web Security Appliance**, click **Browse** to choose a valid XML file to import from a Web Security appliance.
- Step 9** Click **Import**.
- This loads the selected XML file from a Web Security appliance.
- Step 10** Click **Confirm Import**.

## Further Considerations

When creating an identity on the Security Management appliance, you have the option of making it apply only to specific appliances. So for example, if you purchase a Security Management appliance and want to preserve the existing Web Security appliance configurations and the policies that were created for each Web Security appliance, you must load one file into the machine, and then add policies from other machines by hand.

One way to accomplish this is to make a set of identities for each appliance, then have policies which refer to those identities. When the Security Management appliance publishes the configuration, those identities and the policies which refer to them will automatically be removed and disabled. Using this method, you do not have to configure anything manually. This is essentially a ‘per-appliance’ identity.

The only challenge with this method is if you have a default policy or identity that differs between sites. For example, if you have a policy set for “default allow with auth” at one site and a “default deny” at another. At this point you will need to create per-appliance identities and policies just above the default; essentially creating your own “default” policy.

Related Topics

[Table D-6](#) lists each of the topics discussed in this example. Click on the link for details on each topic.

**Table D-6**      *Related Topics for Importing a New Configuration File*

| Feature Name          | Feature Information                                                      |
|-----------------------|--------------------------------------------------------------------------|
| Configuration Masters | <a href="#">`Working with Configuration Masters' section on page 8-3</a> |

Example 7: Customizing Access Policies on Remote Web Security Appliances and Managing Them on a Central Security Management Appliance



Note

This example assumes that you have Configuration 6.3 initialized.

Many customers want to use one Security Management appliance to manage multiple Web Security appliance deployments, where access policy can vary by geographic location due to local laws.

For example, you may need a customized set of rules for employees in China, North America, and Europe, where the access policies can be locally administered.

In this scenario, we explain how to customize access policies for geographic remote Web Security appliances and give local control of the access policy to the local administrator on the Security Management appliance.

With this scenario, you are going to create identities to distinguish users at each of three locations, then create appropriate access policies for the locations. Next you need to add the identity of the location to the location's customized access policy. When users are tagged to this identity, policies that are part of this identity will be applied to this set of users. Finally, you will need to create delegated administrators to maintain the local access policies.

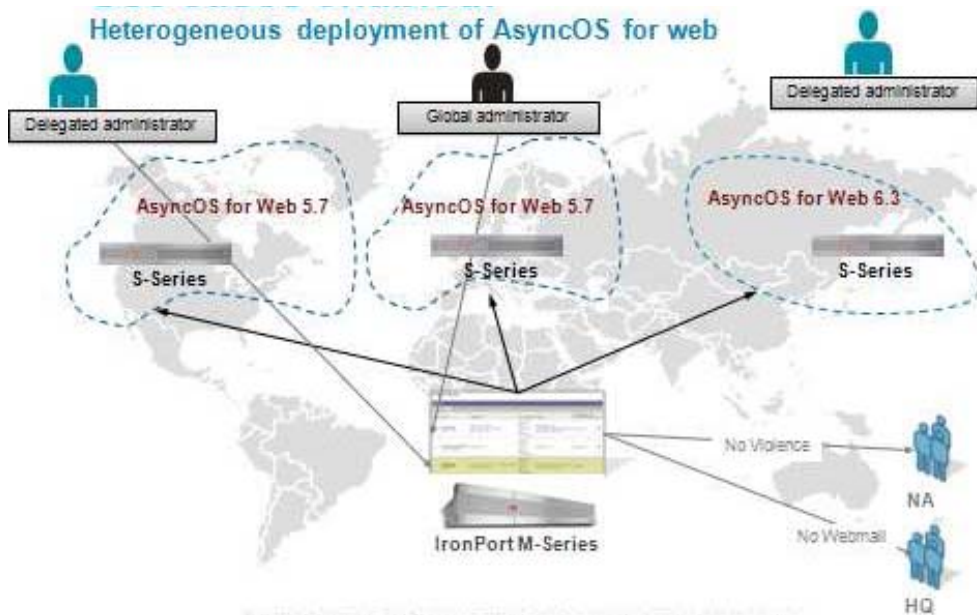
To do this, perform the following:

|        | Action                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <a href="#">Set Up the Access Rules</a>             | <p>For this example, we will set up three access rules and put these rules into access policies as appropriate:</p> <ul style="list-style-type: none"> <li>• The social networking access rule restricts access to social networking sites.</li> <li>• The weapons and violence access rule restricts access to weapons and violence sites.</li> <li>• The web-based e-mail access rule restricts access to web-based e-mail.</li> </ul> |
| Step 2 | <a href="#">Decide Where the Access Rules Apply</a> | <p>The social networking access rule applies to all sites. Place this rule into the global access policy when possible.</p> <p>The weapons and violence rule applies to the North American site. Place this rule into the NA access policy. The web-based email access rule applies to headquarters site in Europe. Place this rule into the HQ access policy.</p>                                                                       |
| Step 3 | <a href="#">Create the Identities</a>               | <p>This step allows you to create an identity for the people the policy applies to and the Web Security appliance that they use.</p> <p>Each of the sites is identified by the corresponding Web Security appliance and the subnet where the users are connected.</p>                                                                                                                                                                    |

|        | Action                                                    | Description                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | Create A Custom URL Category for Configuration Master 5.7 | Because there is no social networking URL category in AsyncOS 5.7 as there is in 6.3, we need to create a custom URL category in order to make the policy uniform across the Web Security appliances running AsyncOS 5.7 and 6.3.                                                                                                                                            |
| Step 5 | Create the Access Policies and Add Identities             | <p>The global policy forbids to access social networking sites. The North American access policy forbids access to weapons and violence sites. The European access policy forbids access to web-based email.</p> <p>Additionally, you must add the identity to specify who the access policy applies to, and the custom URL category to specify the sites it applies to.</p> |
| Step 6 | Create the Delegated Administrators                       | The local access policies for North America and Europe will be maintained by administrators at the local sites who will be more familiar with the local policies and rules.                                                                                                                                                                                                  |

Figure D-2 illustrates how this delegation will work.



**Figure D-2 Delegated Administration**

## Set Up the Access Rules

For this example, we will set up three access rules and put these rules into access policies as appropriate:

- The social networking access rule restricts access to social networking sites.
- The weapons and violence access rule restricts access to weapons and violence sites.
- The web-based e-mail access rule restricts access to web-based e-mail.

**Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.

The Security Appliances page appears.

Figure D-3 The Security Appliances Page

**Security Appliances**

| Centralized Service Status   |                           |
|------------------------------|---------------------------|
| Configuration Manager (Web): | Enabled, using 0 licenses |
| Spam Quarantine:             | Service disabled          |
| Reporting:                   | Enabled, using 0 licenses |
| Tracking:                    | Enabled, using 0 licenses |

**Security Appliances**

**Email**

[Add Email Appliance...](#)

No appliances have been added.

**Web**

[Add Web Appliance...](#)

No appliances have been added.

**Step 2** Click **Add Web Appliance** button to display the Add Web Security Appliance page

Figure D-4 The Add Web Security Appliance Page

**Add Web Security Appliance**

| Web Security Appliance Settings |                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Name:                 | <input type="text"/>                                                                                                                                                                     |
| IP Address:                     | <input type="text"/>                                                                                                                                                                     |
| WSA Centralized Services:       | <input checked="" type="checkbox"/> Centralized Configuration Manager<br><input checked="" type="checkbox"/> Centralized Reporting                                                       |
| Connection Status:              | Not established.<br>Establish an SSH connection for Centralized Web Services.<br><a href="#">Establish Connection...</a> <a href="#">Test Connection</a>                                 |
| Assign Configuration Master: ?  | More assignment options may be enabled once an SSH connection is established.<br><input checked="" type="radio"/> Not Assigned<br><input type="radio"/> 5.7<br><input type="radio"/> 7.1 |

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

**Step 3** In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Cisco IronPort appliance.

In this example, the appliance names will be China, HQ and NA.



**Note**

A DNS name may be entered in the IP Address text field, however, it will be immediately resolved to an IP address when you click **Submit**.

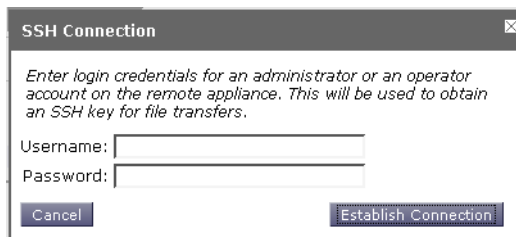
- Step 4** Select the services that you want to use when managing the Cisco IronPort appliance.



**Note** You can select a service only if you have enabled it on the Security Management appliance.

- Step 5** Click **Establish Connection**.  
The SSH Connection dialog box appears.

**Figure D-5 The SSH Connection Dialog Box**



- Step 6** In the Username and Password text fields, type in the login credentials for an administrator account on the Cisco IronPort appliance.



**Note** You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

- Step 7** Click **Establish Connection** to establish the connection for the monitoring services.
- Step 8** Click **Test Connection** to verify that the monitoring services on the remote appliance have been correctly configured and are compatible.
- Step 9** If you are adding a Web Security appliance, choose the Configuration Master to which you want to assign the appliance.

Each Configuration Master contains the configuration for a version of the Web Security appliances. The Security Management appliance can publish a Configuration Master only to a Web Security appliance that is running a compatible version of AsyncOS (for example, if the Web Security appliance is running AsyncOS 6.3, then choose 6.3.0 as the Configuration Master). You can

also assign the Web Security appliance later by choosing **Web > Utilities > Configuration Masters** (see the [`Associating Web Security Appliances to Configuration Masters`](#) section on page 8).

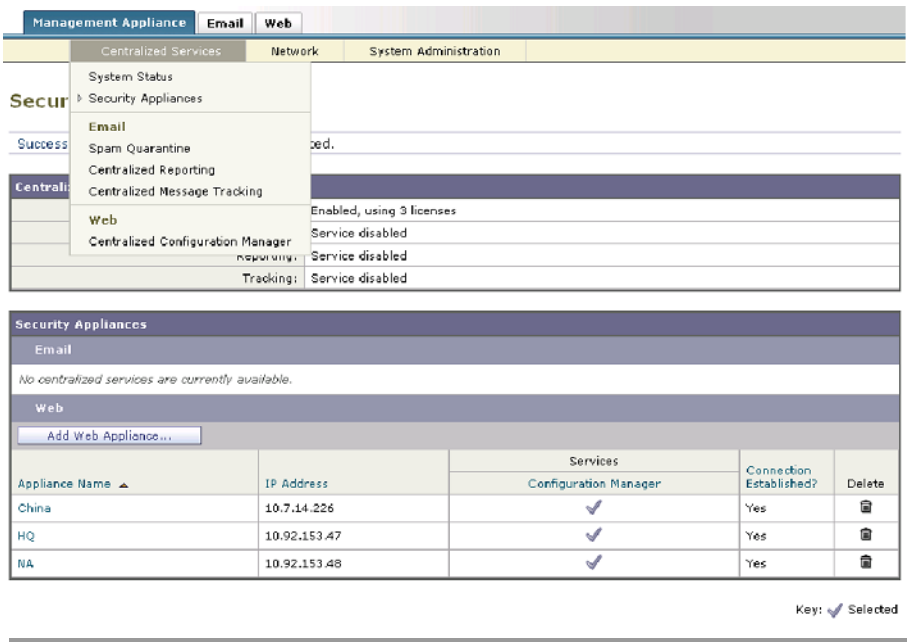
For more information about Configuration Masters and managing Web Security appliances, see [Chapter 8, `Managing Web Security Appliances.`](#)

**Step 10** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.

The Security Appliances page shows the managed appliances that you have added. Check marks indicate the enabled services, and the Connection Established? column shows whether or not the connection for monitoring services is properly configured.

[Figure D-6](#) displays the newly added appliances that will be managed.

**Figure D-6** Web Security Appliances Added for Delegated Administration



## Decide Where the Access Rules Apply

In this step, we are defining the following global access policy that will apply to everyone in the company.

- The Social Networking Rule  
This access policy applies to all sites.
- The Weapons and Violence Rule  
This policy is local to the North America branch.
- The Web-based E-mail Rule  
This policy is local to the HQ branch.



### Note

Before you begin setting up access policies, make sure that the Centralized Web Configuration Manager is enabled.

- 
- Step 1** On the Security Management appliance, choose **Web > Configuration Manager 7.1 > Access Policies**.
  - Step 2** Click **Add Policy**.
  - Step 3** On the Access Policy:Add Group window, type **Social Networking Rule** and apply this policy to all sites.
  - Step 4** Click **Submit**.
  - Step 5** Go back to **Web > Configuration Manager 7.1 > Access Policies** and click on **Add Policy**.
  - Step 6** On the Access Policy:Add Group window, type **Weapons and Violence Rule** and apply this policy to the North American site.
  - Step 7** Click **Submit**.
  - Step 8** And finally, go back to **Web > Configuration Manager 7.1 > Access Policies** and click on **Add Policy**.
  - Step 9** On the Access Policy:Add Group window, type **Web-based Email Rule** and apply this policy to the HQ site.
  - Step 10** Click **Submit**.
-

## Create the Identities

This step allows you to create an identity for the people the policy applies to and the Web Security appliance that they use. Each of the sites is identified by the corresponding Web Security appliance and the subnet where the users are connected.

- Step 1** Choose **Web > Configuration Master 5.7 > Identities > Add Identities** to create the China branch Identity.

Management Appliance

Email

Web

Utilities

Configuration Master 5.7

Configuration Master 6.3

Identities

Web Security Manager

Identities

Decryption Policies

Routing Policies

Access Policies

Success — Item was added

Client / Transaction

Proxy Bypass

Custom URL Categories

Time Ranges

Add Identity...

Order

Membership Definition

Global Identity Policy

Exempt from authentication

End-User Acknowledgement

Delete

Required

Authentication: Enabled Disabled Policy Disabled

- Step 2** Choose **Web > Configuration Master 5.7 > Identities > Add Identities** to create the North America Identity.

The Weapons and Violence Rule policy only applies to the North America site. The Web Security appliance at the North America site is running AsyncOS 5.7.

- Step 3** In the Identity Settings text field, type **NA identity**.

- Step 4** Click **All Managed Appliances** next to Include these Appliances, to restrict the identity to the appliance in the North America site.

| Management Appliance | Email                    | Web                      |
|----------------------|--------------------------|--------------------------|
| Utilities            | Configuration Master 5.7 | Configuration Master 6.3 |

## Identities: Add Identity

| Identity Settings                                          |                                                   |
|------------------------------------------------------------|---------------------------------------------------|
| <input checked="" type="checkbox"/> <b>Enable Identity</b> |                                                   |
| Name: ?                                                    | NA identity<br><small>(e.g. my IT policy)</small> |
| Description:                                               | The identity for the North America branch.        |
| Insert Above:                                              | 1 (HR identity) ▼                                 |

| Membership Definition                                                                                                                     |                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small> |                                                                                                                                  |
| Include These Appliances:                                                                                                                 | All Managed Appliances                                                                                                           |
| Define Members by Subnet:                                                                                                                 | <div></div><br><small>(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)</small>                                                     |
| Authentication Realm:                                                                                                                     | No Authentication Required ▼<br><small>Authorization of specific users and groups is defined in subsequent policy layers</small> |
| ▶ Advanced                                                                                                                                | <small>Define additional group membership criteria.</small>                                                                      |

**Step 5** Choose **Web > Identity Policies > Managed Appliances**.

**Step 6** Check the checkbox next to **NA**.

In this example, the group of users is everyone on the 10.10.3.0/24 subnet.

| Identity Settings                                          |                                                   |
|------------------------------------------------------------|---------------------------------------------------|
| <input checked="" type="checkbox"/> <b>Enable Identity</b> |                                                   |
| Name: ?                                                    | NA identity<br><small>(e.g. my IT policy)</small> |
| Description:                                               | The identity for the North America branch.        |
| Insert Above:                                              | 1 (HR identity) ▼                                 |

| Membership Definition                                                                                                                     |                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small> |                                                                                                                                  |
| Include These Appliances:                                                                                                                 | NA                                                                                                                               |
| Define Members by Subnet:                                                                                                                 | 10.10.3.0/24<br><small>(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)</small>                                                    |
| Authentication Realm:                                                                                                                     | No Authentication Required ▼<br><small>Authorization of specific users and groups is defined in subsequent policy layers</small> |
| ▶ Advanced                                                                                                                                | <small>Define additional group membership criteria.</small>                                                                      |

- Step 7

Create a new identity for **HQ** as you did for NA (steps 2 - 6).

Check the checkbox for the **HQ** Web Security appliance for this identity. The group of users in this example is everyone on the 10.10.1.0/24 subnet.

You now have two identities created as shown in [Figure D-7](#).

Figure D-7 Created Identities

Management Appliance
Email
Web

Utilities
Configuration Master 5.7
Configuration Master 6.3

Identities

Success — Your changes have been committed.

Client / Transaction Identity Definitions

Add Identity...

| Order                                                       | Membership Definition                                                                       | End-User Acknowledgement | Delete |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------|--------------------------|--------|
| 1                                                           | <b>HQ identity</b><br>Appliances: HQ<br>Subnets: 10.10.1.0/24<br>Exempt from authentication | (global policy)          |        |
| 2                                                           | <b>NA identity</b><br>Appliances: NA<br>Subnets: 10.10.3.0/24<br>Exempt from authentication | (global policy)          |        |
| <b>Global Identity Policy</b><br>Exempt from authentication |                                                                                             | Required                 |        |

Authentication:
 Enabled
 Disabled
Policy Disabled

Create A Custom URL Category for Configuration Master 5.7

- Now we have to create a custom URL category because while the Social Networking URL category is available on AsyncOS 6.3, it is not on available in AsyncOS 5.7.
- The Social Networking custom category will contain the following sites:
- myspace.com
  - facebook.com
  - linkedin.com
  - twitter.com



- badoo.com

**Step 1** On the Security Management appliance, choose **Web > Configuration Master 7.1 > Custom URL Categories**.

The Custom URL categories page appears.

**Step 2** Click **Add Custom Category** to create the Social Networking category for 5.7.

**Figure D-8 Creating a Custom URL Category**

**Custom URL Categories: Add Category**

**Edit Custom URL Category**

Category Name:

List Order:

Sites:

[Sort URLs](#)  
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g., example.com, .example.com, 10.1.1.1, 10.1.1.0/24)

Advanced

Regular Expressions (Access Policies Only):

Enter one regular expression per line.

**Step 3** Enter the following settings in the appropriate fields to create, or edit the custom URL category.

- **Category Name**—Enter a name for the URL category. This name appears when you configure URL filtering for policy groups.
- **Sites**—Enter the domain name that belong in the Social Networking category.

You can enter multiple addresses separated by line breaks or commas. For this example we are using the following domains:

- myspace.com
- facebook.com
- linkedin.com
- twitter.com
- badoo.com

Figure D-9 Custom URL Categories

Management Appliance

Email

Web

Utilities

Configuration Master 5.7

Configuration Master 6.3

Custom URL Categories: Add Category

Edit Custom URL Category

Category Name:

Social Networking

List Order:

1

Sites: (?)

.myspace.com

.facebook.com

.linkedin.com

.twitter.com

.badoo.com

(e.g. example.com, .example.com, 10.1.1.1, 10.1.1.0/24)

Advanced

Match specific URLs by regular expressions.

Cancel

Submit

**Step 4** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes on the appliance.

Create the Access Policies and Add Identities

In this step we are going to create an access policy for all sites to restrict access to social networking sites. We need to create three policies:

- The China Policy
- The NA policy
- The HQ policy

The Web Security appliance in the China branch, is only running with Configuration Master 6.3. The only access policy rule for the China branch is the rule forbidding access to social networking sites. The social networking category is included in the set of URL categories in Configuration Master 6.3, so we only need to ensure that social networking has been selected as a URL Category that is forbidden.

**Step 1** On the Security Management appliance, choose **Web > Configuration Master 6.3 > Access Policies**.

- Step 2** Click on the link in the **URL Categories** column to modify the Global access policy.
- Step 3** Make sure that the Social Networking has been selected and has an assigned identity as blocked.

|                     |   |  |   |   |
|---------------------|---|--|---|---|
| Shopping            | ✓ |  |   | — |
| Social Networking   |   |  | ✓ | — |
| Social Science      | ✓ |  |   | — |
| Society and Culture | ✓ |  |   | — |

The Web Security appliance in the NA branch is running AsyncOS 5.7. The NA access policy must enforce two rules.

- A local rule forbidding access to weapons and violence sites.
- A rule forbidding access to social networking sites.

Because the Social Networking category is not included to 5.7, we need to create the social networking custom URL category to ensure that social networking is forbidden.

- Step 4** On the Security Management appliance, choose **Web > Configuration Master 5.7> Access Policies**.
- Step 5** Click **Add Policy**.
- Step 6** On the **Access Policies: Add Policy** page do the following:
- In the Policy Setting section check the **Enable Policy** checkbox.
  - Type **NA policy** in the Policy Name text field
  - In the Policy Member Definition section, select **NA Identity** from the drop-down list.
- Step 7** Click **Submit**.
- After you click **Submit**, you are returned to the Access Policies Page.
- Step 8** On the Access Policies page, in the NA access policy row, click the **global policy** link in the **URL Categories** column.
- Step 9** Make sure that the Weapons and Violence URL categories are selected for this access policy. Additionally, make sure that **Social Networking** custom URL category is blocked.

|                  |  |  |  |  |
|------------------|--|--|--|--|
| Travel           |  |  |  |  |
| Violence         |  |  |  |  |
| Weapons          |  |  |  |  |
| Web-based E-mail |  |  |  |  |

Finally, we need to deal with the HQ branch policy. The Web Security appliance in the HQ branch is running AsyncOS 5.7. The NA access policy must enforce two rules:

- The local rule forbidding access to web-base e-mail sites.
- The rule forbidding access to social networking sites.

Because the Social Networking category is not included to 5.7, we need to create the Social Networking custom URL category to ensure that social networking is forbidden.

**Step 10** On the Security Management appliance, choose **Web > Configuration Master 5.7> Access Policies**.

**Step 11** Click **Add Policy**.

**Step 12** On the **Access Policies: Add Policy** page do the following:

- In the Policy Setting section check the **Enable Policy** checkbox.
- Type **HQpolicy** in the Policy Name text field
- In the Policy Member Definition section, select **HQ Identity** from the drop-down list.

**Step 13** Click **Submit**.

After you click **Submit**, you are returned to the Access Policies Page.

**Step 14** On the Access Policies page, in the HQ access policy row, click the **global policy** link in the **URL Categories** column.

**Step 15** Make sure that the **Social Networking** custom URL category is blocked. Additionally, make sure that the **Web-based Email** category is blocked.

|                  |  |  |  |  |
|------------------|--|--|--|--|
| Travel           |  |  |  |  |
| Violence         |  |  |  |  |
| Weapons          |  |  |  |  |
| Web-based E-mail |  |  |  |  |

At this point you have now completed substituting the new social networking policy for the default social networking policy at the headquarters Web Security appliances.

**Figure D-10** Completed Policies for Example 7

Management Appliance

Email

Web

Utilities

Configuration Master 5.7

Configuration Master 6.3

# Access Policies

Policies

Add Policy...

View: All Policies

| Order | Group                                     | Applications                                          | URL Categories                                                      | Objects               | Web Reputation and Anti-Malware Filtering | Delete |
|-------|-------------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------|-----------------------|-------------------------------------------|--------|
| 1     | NA access policy<br>Identity: NA identity | (global policy)                                       | Redirect: 0<br>Allow: 0<br>Monitor: 51<br>Block: 3<br>Time-Based: 0 | (global policy)       | (global policy)                           |        |
| 2     | HQ access policy<br>Identity: HQ identity | (global policy)                                       | Redirect: 0<br>Allow: 0<br>Monitor: 52<br>Block: 2<br>Time-Based: 0 | (global policy)       | (global policy)                           |        |
|       | Global Policy<br>Identity: All            | Allow: FTP over HTTP, HTTP<br>Allow: Ports 20, 21,... | Redirect: 0<br>Allow: 0<br>Monitor: 53<br>Block: 1<br>Time-Based: 0 | Object Max Size: None | (enabled)                                 |        |

Authentication: Enabled Disabled

Policy Disabled

## Create the Delegated Administrators

Now you must add the delegated administrators. To do this we must create a web user role for the delegated administrator that assigns the access policies that they can manage.

To define user roles:

- Step 1** On the Security Management appliance, choose **Management Appliance > System Administration > User Roles**.
- Step 2** Click **Add Web User Role**.  
This allows us to add the NA branch user role.
- Step 3** On the Edit Web User Roles page, type **na\_admin\_role** in the Name text field.
- Step 4** Click **Submit**.  
The User Roles page appears.

**Step 5** Click on **Access policies** in the **na\_admin\_role** row under **Configuration Master 5.7**.

Management Appliance

Email

Web

Centralized Services

Network

System Administration

User Roles

Success — Your changes have been committed.

User Roles for Delegated Administration of Web Policies

Add User Role...

| Role Name     | Privileges                                     |                                                | Description                                                 | Assigned Users | Delete |
|---------------|------------------------------------------------|------------------------------------------------|-------------------------------------------------------------|----------------|--------|
|               | Configuration Master 5.7                       | Configuration Master 6.3                       |                                                             |                |        |
| na_admin_role | Access Policies: 0<br>Custom URL Categories: 0 | Access Policies: 0<br>Custom URL Categories: 0 | This is the role for the NA branch delegated administrator. |                |        |

The **Edit Access Policy Privileges: na\_admin\_role** page appears.

**Step 6** Check the checkbox next to NA Access Policy to select the NA access policy to the user role for the NA delegated administrator.

At this point, we will not add the social networking custom URL to the NA branch user role. This is a shared URL category. Changing it at one site would affect all sites. We will leave this category under the control of the main administrator. The NA branch User Role is now complete.

Now that we have a user role for the delegated user, we can create the NA branch delegated administrator.

**Step 7** On the Security Management appliance, choose **Management Appliance > System Administration > Users**.

**Step 8** Click **Add User**.

**Step 9** Click on the **Custom Roles** radio button and select the **na\_admin\_role** in the window below Custom Roles.

**Step 10** Click **Submit**.

This now gives you a NA Delegated Administrator.

Options ▾ Help and Support

Management Appliance Email Web

Centralized Services Network System Administration

## Users

Success — Your changes have been committed.

| Users                       |               |                |        |
|-----------------------------|---------------|----------------|--------|
| <a href="#">Add User...</a> |               |                |        |
| User Name                   | Full Name     | User Role      | Delete |
| na_admin                    | Joe Admin     | na_admin_role* |        |
| admin                       | Administrator | Administrator  |        |

\* Custom User Role for delegated administration of web policies.

| External Authentication                 |         |
|-----------------------------------------|---------|
| External Authentication:                | Enabled |
| Authentication Type:                    | LDAP    |
| <a href="#">Edit Global Settings...</a> |         |

Now we need to create a new user role to have an HQ delegated administrator.

- Step 11** On the Security Management appliance, choose **Management Appliance > System Administration > Users**.
- Step 12** Click **Add Users**.
- Step 13** On the Edit User Roles page, type **hq\_admin\_role** in the Name text field.
- Step 14** Click **Submit**.
- Step 15** On the User Roles page, click on **Access policies** in the **hq\_admin\_role** row under **Configuration Master 5.7**.
- Step 16** On the Edit Access Policies page, check the Include checkbox to allow the HQ delegated administrator to manage the HQ access policy.

Edit Access Policy Privileges: hq\_admin\_role

Access Policies (Configuration Master 5.7)

| Include                             | Order | Policies                                  | Existing User Roles with Edit Access |
|-------------------------------------|-------|-------------------------------------------|--------------------------------------|
| <input checked="" type="checkbox"/> | 1     | HQ access policy<br>Identity: HQ identity |                                      |
| <input type="checkbox"/>            | 2     | NA access policy<br>Identity: NA identity | na_admin_role                        |
| <input type="checkbox"/>            | Last  | Global Policy<br>Identity: All            |                                      |

Cancel

Submit

- Step 17
- Click **Submit**.
- Step 18
- On the Security Management appliance, choose **Management Appliance > System Administration > Users**.
- Step 19
- Click **Add User**.
- Step 20
- Click on the **Custom Roles** radio button and select the **hq\_admin\_role** in the window below Custom Roles.
- This assigns the HQ administrator role to the HQ administrator.
- Step 21
- Click **Submit**.

Figure D-11 show the Users table displaying the assigned delegated administrators.

Figure D-11 Assigned Delegated Administrators

Users

Success — Your changes have been committed.

Users

Add User...

| User Name | Full Name     | User Role      | Delete |
|-----------|---------------|----------------|--------|
| hq_amin   | Jacques Admin | hq_admin_role* |        |
| na_admin  | Joe Admin     | na_admin_role* |        |
| admin     | Administrator | Administrator  |        |

\* Custom User Role for delegated administration of web policies.

External Authentication

External Authentication: Enabled

Authentication Type: LDAP

Edit Global Settings...

You are done!



At this point you have created identities to distinguish users at each of three locations.

You then created appropriate access policies for the locations and added the identity of the location to the location’s customized access policy.

You then created a URL category in order to add a category that does not appear in AsyncOS 5.7.

And finally you have created delegated administrators to maintain the local access policies.

## Related Topics

[Table D-7](#) lists each of the topics discussed in this example. Click on the link for details on each topic.

**Table D-7**      ***Related Topics for Customizing Access Policies***

| Feature Name               | Feature Information                              |
|----------------------------|--------------------------------------------------|
| User Page                  | <a href="#">Users Page, page 5-16</a>            |
| User Details Page          | <a href="#">User Details Page, page 5-20</a>     |
| Custom URL Categories Page | <a href="#">Custom URL Categories, page 5-33</a> |





## APPENDIX **E**

# Interactive Columns

---

This appendix describes all of the available columns for the Management Appliance, Web, and Email appliance report pages, and their meaning.

- [Interactive Columns for the Centralized Web Reporting Pages, page E-1](#)
- [Interactive Columns for the Centralized Email Reporting Pages, page E-5](#)

## Interactive Columns for the Centralized Web Reporting Pages

This section describes the interactive columns that are available on various Web Security appliance report pages.



### Note

Not every column is available for every report page. Click on the column link for each Web Reporting page to view the columns available for that specific report page. Additionally, some of the results the columns provide a link to the [Web Tracking Page](#) for that result.

---

**Table E-1**      *Interactive Column Descriptions for Centralized Web Reporting Pages*

| Column Name                 | Description                                                                                                                |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Domain or Realm             | The domain or realm of the user displayed in text format.                                                                  |
| UserID or Client IP         | The user ID or client IP of the user displayed in text format.                                                             |
| Bandwidth Used              | The amount of bandwidth that is used by a particular user or action. Bandwidth units are displayed in Bytes or percentage. |
| Bandwidth Saved by Blocking | The amount of bandwidth that has been saved due to blocking certain transactions. Bandwidth units are displayed in Bytes   |

**Table E-1**      **Interactive Column Descriptions for Centralized Web Reporting Pages**

| Column Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Spent             | <p>The amount of time spent on a web page. For purposes of investigating a user, the time spent by the user on each URL category. When tracking a URL, the time spent by each user on that specific URL.</p> <p>Once a transaction event is tagged as ‘viewed’, that is, a user goes to a particular URL, a ‘Time Spent’ value will start to be calculated and added as a field in the web reporting table.</p> <p>To calculate the time spent, AsyncOS assigns each active user with 60 seconds of time for activity during a minute. At the end of the minute, the time spent by each user is evenly distributed among the different domains the user visited. For example, if a user goes to four different domains in an active minute, the user is considered to have spent 15 seconds at each domain.</p> <p>For the purposes of the time spent value, considering the following notes:</p> <ul style="list-style-type: none"> <li>• An active user is defined as a username or IP address that sends HTTP traffic through the appliance and has gone to a website that AsyncOS considers to be a “page view.”</li> <li>• AsyncOS defines a page view as an HTTP request initiated by the user, as opposed to a request initiated by the client application. AsyncOS uses a heuristic algorithm to make a best effort guess to identify user page views.</li> </ul> <p>Units are displayed in HH:MM format.</p> |
| Allowed URL Category   | The number and type of categories that have been allowed. Units displayed in transaction type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Monitored URL Category | The number and type of categories that are being monitored. Units displayed in transaction type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Warned URL Category    | The number and type of categories that have initiated a warning. Units displayed in transaction type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Table E-1**      **Interactive Column Descriptions for Centralized Web Reporting Pages**

| Column Name                                | Description                                                                                         |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Blocked by URL Category                    | The transaction that has been blocked due to URL Category. Units displayed in transaction type.     |
| Blocked by Application or Application Type | The application that has been blocked due to application type. Units displayed in transaction type. |
| Blocked by Web Reputation                  | The transaction that has been blocked due to web reputation. Units displayed in transaction type.   |
| Blocked by Anti-Malware                    | The transactions blocked by Anti-Malware. Units displayed in transaction type.                      |
| Other Blocked Transactions                 | All other transactions that have been blocked. Units displayed in transaction type.                 |
| Transactions with Bandwidth Limit          | The number of transactions that have a bandwidth limit.                                             |
| Transactions without Bandwidth Limit       | The number of transactions that do not have a bandwidth limit.                                      |
| Transactions Blocked by Application        | The number of transactions blocked by a specific application type.                                  |
| Warned Transactions                        | All transactions that rendered a warning to the user. Units displayed in transaction type.          |
| Transactions Completed                     | The transactions completed by a user. Units displayed in transaction type.                          |
| Transactions Blocked                       | All transactions that have been blocked. Units displayed in transaction type.                       |
| Total Transactions                         | The total number of transactions that have occurred.                                                |

# Interactive Columns for the Centralized Email Reporting Pages

This section describes the interactive columns that are available on various Centralized Email Security appliance report pages.

**Table E-2**      ***Interactive Column Descriptions***

| Column Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Incoming Mail Details</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 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,                                                                                                                                                                                                                                                                                                                                                                                                           |
| Total Attempted                 | All accepted and blocked connections attempted.                                                                                                                                                                                                                                                                                                                                                                                     |
| 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. |

**Table E-2**      **Interactive Column Descriptions**

| Column Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stopped by Reputation Filtering                     | <p>The value for Stopped by Reputation Filtering is calculated based on several factors:</p> <ul style="list-style-type: none"> <li>• Number of “throttled” messages from this sender</li> <li>• Number of rejected or TCP refused connections (may be a partial count)</li> <li>• A conservative multiplier for the number of messages per connection</li> </ul> <p>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”; that is, at least this many messages were stopped.</p> <p> <b>Note</b>      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 limited due to load.</p> |
| Spam Detected                                       | Any spam that has been detected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Virus Detected                                      | Any viruses that have been detected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Stopped by Content Filter                           | The total count of messages that were stopped by a content filter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Total Threat                                        | Total number of threat messages (stopped by reputation, stopped as invalid recipient, spam, plus virus)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Clean                                               | All clean messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DNS Verified                                        | All domain names that have been verified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SBRS                                                | The Sender Base Reputation Score.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Last Sender Group                                   | The last valid sender group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Total Attempted                                     | Total number of incoming mail messages that were attempted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>User Mail Flow Details (Internal Users Page)</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Incoming Spam Detected                              | All incoming spam that is detected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



**Table E-2**      **Interactive Column Descriptions**

| Column Name                                                        | Description                                                                        |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Incoming Virus Detected                                            | The incoming virus that has been detected.                                         |
| Incoming Content Filter Matches                                    | The incoming content filter matches that have been detected.                       |
| Incoming Stopped by Content Filter                                 | The Incoming messages that were stopped due to content filters that have been set. |
| Incoming Clean                                                     | All incoming clean messages.                                                       |
| Outgoing Spam Detected                                             | The outgoing spam that was detected.                                               |
| Outgoing Virus Detected                                            | The outgoing viruses that have been detected.                                      |
| Outgoing Content Filter Matches                                    | The outgoing content filter matches that have been detected.                       |
| Outgoing Stopped by Content Filter                                 | The outgoing messages that were stopped due to content filters that have been set. |
| Outgoing Clean                                                     | All outgoing clean messages.                                                       |
| <b>Incoming and Outgoing TLS Connections: TLS Connections Page</b> |                                                                                    |
| Required TLS: Failed                                               | All required TLS connections that failed.                                          |
| Required TLS: Successful                                           | All required TLS connections that are successful.                                  |
| Preferred TLS: Failed                                              | All preferred TLS connections that failed.                                         |
| Preferred TLS: Successful                                          | All preferred TLS connections that are successful.                                 |
| Total Connections                                                  | Total number of TLS connections.                                                   |
| Total Messages                                                     | The total number of TLS messages.                                                  |
| <b>Virus Outbreaks</b>                                             |                                                                                    |
| Outbreak Name                                                      | The name of the outbreak.                                                          |
| Outbreak ID                                                        | The outbreak ID.                                                                   |
| First Seen Globally                                                | The first time the virus has been seen globally.                                   |
| Protection Time                                                    | The time the virus has been protected.                                             |
| Quarantined Messages                                               | Messages related to the quarantine.                                                |





## APPENDIX **F**

# Cisco IronPort End User License Agreement

---

This appendix contains the following section:

- [Cisco IronPort Systems, LLC Software License Agreement, page F-1](#)

## Cisco IronPort Systems, LLC Software License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”) FOR THE LICENSE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY, COLLECTIVELY, THE “COMPANY”) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THE FOLLOWING AGREEMENT BETWEEN CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION (“IRONPORT”) AND COMPANY (COLLECTIVELY, THE “PARTIES”). BY CLICKING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED. IF YOU OR THE COMPANY YOU REPRESENT (COLLECTIVELY, “COMPANY”) DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK THE CANCEL BUTTON OR ENTER “N” WHEN

PROMPTED AND PROMPTLY (BUT NO LATER THAT THIRTY (30) DAYS OF THE DELIVERY DATE, AS DEFINED BELOW) NOTIFY IRONPORT, OR THE RESELLER FROM WHOM YOU RECEIVED THE SOFTWARE, FOR A FULL REFUND OF THE PRICE PAID FOR THE SOFTWARE.

## 1. DEFINITIONS

1.1 “Company Service” means the Company’s email or internet services provided to End Users for the purposes of conducting Company’s internal business and which are enabled via Company’s products as described in the purchase agreement, evaluation agreement, beta or pre-release agreement, purchase order, sales quote or other similar agreement between the Company and IronPort or its reseller (“Agreement”) and the applicable user interface and IronPort’s standard system guide documentation that outlines the system architecture and its interfaces (collectively, the “License Documentation”).

1.2 “End User” means the employee, contractor or other agent authorized by Company to access to the Internet or use email services via the Company Service.

1.3 “Service(s)” means (i) the provision of the Software functionality, including Updates and Upgrades, and (ii) the provision of support by IronPort or its reseller, as the case may be.

1.4 “Software” means: (i) IronPort’s proprietary software licensed by IronPort to Company along with IronPort’s hardware products; (ii) any software provided by IronPort’s third-party licensors that is licensed to Company to be implemented for use with IronPort’s hardware products; (iii) any other IronPort software module(s) licensed by IronPort to Company along with IronPort’s hardware products; and (iv) any and all Updates and Upgrades thereto.

1.5 “Updates” means minor updates, error corrections and bug fixes that do not add significant new functions to the Software, and that are released by IronPort or its third party licensors. Updates are designated by an increase to the Software’s release number to the right of the decimal point (e.g., Software 1.0 to Software 1.1). The term Updates specifically excludes Upgrades or new software versions marketed and licensed by IronPort or its third party licensors as a separate product.

1.6 “Upgrade(s)” means revisions to the Software, which add new enhancements to existing functionality, if and when it is released by IronPort or its third party licensors, in their sole discretion. Upgrades are designated by an increase in the Software’s release number, located to the left of the decimal point (e.g., Software

1.x to Software 2.0). In no event shall Upgrades include any new versions of the Software marketed and licensed by IronPort or its third party licensors as a separate product.

## 2. LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

2.1 License of Software. By using the Software and the License Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, IronPort hereby grants to Company a non-exclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on IronPort's hardware products, solely in connection with the provision of the Company Service to End Users. The duration and scope of this license(s) is further defined in the License Documentation. Except as expressly provided herein, no right, title or interest in any Software is granted to the Company by IronPort, IronPort's resellers or their respective licensors. This license and any Services are co-terminus.

2.2 Consent and License to Use Data. Subject to Section 8 hereof, and subject to the IronPort Privacy Statement at <http://www.ironport.com/privacy.html>, as the same may be amended from time to time by IronPort with notice to Company, Company hereby consents and grants to IronPort a license to collect and use the data from the Company as described in the License Documentation, as the same may be updated from time to time by IronPort ("Data"). To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content. Notwithstanding the foregoing, Company may terminate IronPort's right to collect and use Data at any time upon prior written or electronic notification, provided that the Software or components of the Software may not be available to Company if such right is terminated.

3. CONFIDENTIALITY. Each Party agrees to hold in confidence all Confidential Information of the other Party to the same extent that it protects its own similar Confidential Information (and in no event using less than a reasonable degree of care) and to use such Confidential Information only as permitted under this Agreement. For purposes of this Agreement "Confidential Information" means information of a party marked "Confidential" or information reasonably considered by the disclosing Party to be of a proprietary or confidential nature; provided that the Data, the Software, information disclosed in design reviews and any pre-production releases of the Software provided by IronPort is expressly designated Confidential Information whether or not marked as such.

4. **PROPRIETARY RIGHTS; OWNERSHIP.** Title to and ownership of the Software and other materials and all associated Intellectual Property Rights (as defined below) related to the foregoing provided by IronPort or its reseller to Company will remain the exclusive property of IronPort and/or its superior licensors. Company and its employees and agents will not remove or alter any trademarks, or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software or other materials delivered to Company by IronPort or its reseller. Company will not modify, transfer, resell for profit, distribute, copy, enhance, adapt, translate, decompile, reverse engineer, disassemble, or otherwise determine, or attempt to derive source code for any Software or any internal data files generated by the Software or to create any derivative works based on the Software or the License Documentation, and agrees not to permit or authorize anyone else to do so. Unless otherwise agreed in writing, any programs, inventions, concepts, documentation, specifications or other written or graphical materials and media created or developed by IronPort or its superior licensors during the course of its performance of this Agreement, or any related consulting or professional service agreements, including all copyrights, database rights, patents, trade secrets, trademark, moral rights, or other intellectual property rights (“Intellectual Property Right(s)”) associated with the performance of such work shall belong exclusively to IronPort or its superior licensors and shall, in no way be considered a work made for hire for Company within the meaning of Title 17 of the United States Code (Copyright Act of 1976).

#### 5. LIMITED WARRANTY AND WARRANTY DISCLAIMERS

5.1 **Limited Warranty.** IronPort warrants to Company that the Software, when properly installed and properly used, will substantially conform to the specifications in the License Documentation for a period of ninety (90) days from the delivery date or the period set forth in the License Documentation, whichever is longer (“Warranty Period”). **FOR ANY BREACH OF THE WARRANTY CONTAINED IN THIS SECTION, COMPANY’S EXCLUSIVE REMEDY AND IRONPORT’S ENTIRE LIABILITY, WILL BE PROMPT CORRECTION OF ANY ERROR OR NONCONFORMITY, PROVIDED THAT THE NONCONFORMITY HAS BEEN REPORTED TO IRONPORT AND/OR ITS RESELLER BY COMPANY WITHIN THE WARRANTY PERIOD. THIS WARRANTY IS MADE SOLELY TO COMPANY AND IS NOT TRANSFERABLE TO ANY END USER OR OTHER THIRD PARTY.** IronPort shall have no liability for breach of warranty under this Section or otherwise for breach of this Agreement if such breach arises directly or indirectly out of or in connection with the following: (i) any unauthorized, improper, incomplete or inadequate maintenance or calibration of the Software by Company or any third

party; (ii) any third party hardware software, services or system(s); (iii) any unauthorized modification or alteration of the Software or Services; (iv) any unauthorized or improper use or operation of the Software or Company's failure to comply with any applicable environmental specification; or (v) a failure to install and/or use Updates, Upgrades, fixes or revisions provided by IronPort or its resellers from time to time.

5.2 WARRANTY DISCLAIMER. THE EXPRESS WARRANTIES SET FORTH IN SECTION 5.1 OF THIS AGREEMENT CONSTITUTE THE ONLY PERFORMANCE WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IRONPORT LICENSES THE SOFTWARE AND SERVICES HEREUNDER ON AN "AS IS" BASIS. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, IRONPORT AND ITS SUPERIOR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER IRONPORT NOR ITS THIRD PARTY LICENSORS WARRANT THAT THE SOFTWARE OR SERVICES (1) IS FREE FROM DEFECTS, ERRORS OR BUGS, (2) THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED, OR (3) THAT ANY RESULTS OR INFORMATION THAT IS OR MAY BE DERIVED FROM THE USE OF THE SOFTWARE WILL BE ACCURATE, COMPLETE, RELIABLE AND/OR SECURE.

6. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF SUCH PARTY RECEIVED ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY ARISING UNDER ANY PROVISION OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT, OR OTHER LEGAL THEORY, EXCEED THE TOTAL AMOUNT PAID FOR THE SOFTWARE OR SERVICES DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

7. **TERM AND TERMINATION.** The term of this Agreement shall be as set forth in the License Documentation (the “Term”). If IronPort defaults in the performance of any material provision of this Agreement or the License Documentation, then Company may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day period. If Company defaults in the performance of any material provision of this Agreement or the License Documentation, IronPort may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day notice and without a refund. This Agreement may be terminated by one Party immediately at any time, without notice, upon (i) the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of such Party’s debts, (ii) such other Party making a general assignment for the benefit of creditors, or (iii) such other Party’s dissolution. The license granted in Section 2 will immediately terminate upon this Agreement’s termination or expiration. Within thirty (30) calendar days after termination or expiration of this Agreement, Company will deliver to IronPort or its reseller or destroy all copies of the Software and any other materials or documentation provided to Company by IronPort or its reseller under this Agreement.

8. **U.S. GOVERNMENT RESTRICTED RIGHTS; EXPORT CONTROL.** The Software and accompanying License Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying License Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Company acknowledges that the Software and License Documentation must be exported in accordance with U.S. Export Administration Regulations and diversion contrary to U.S. laws is prohibited. Company represents that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Company export privileges. Company represents that Company will not use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Company acknowledges it is Company’s ultimate responsibility to comply with any and all import and export restrictions, and other applicable laws, in the U.S. or elsewhere, and that IronPort or its reseller has no further responsibility after the initial sale to Company within the original country of sale.



9. MISCELLANEOUS. This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Nothing contained herein shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money) on account of (i) any provision of any present or future law or regulation of the United States or any applicable law that applies to the subject hereof, and (ii) interruptions in the electrical supply, failure of the Internet, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes, or any other cause which is beyond the reasonable control of such party. This Agreement and the License Documentation set forth all rights for the user of the Software and is the entire agreement between the parties and supersedes any other communications with respect to the Software and License Documentation. The terms and conditions of this Agreement will prevail, notwithstanding any variance with the License Documentation or any purchase order or other written instrument submitted by a party, whether formally rejected by the other party or not. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of IronPort, except that IronPort may modify the IronPort Privacy Statement at any time, in its discretion, via notification to Company of such modification that will be posted at <http://www.ironport.com/privacy.html>. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by IronPort or a duly authorized representative of IronPort. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

10. IRONPORT CONTACT INFORMATION. If Company wants to contact IronPort for any reason, please write to IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066, or call or fax us at tel: 650.989.6500 and fax: 650.989.6543.





## INDEX

---

### Symbols

/dev/null, in alias tables [11-3](#)

---

### A

#### Access Policies

- configuring Web Reputation [5-61](#)

active sessions [12-75](#)

#### administration

- distributing [12-40](#)

administration commands [12-1](#)

#### admin password

- changing [2-14](#)

#### advanced file publish

- vs. Configuration Master publish [8-14](#)

alertlisting [12-84](#)

#### alerts

- classifications [12-77](#)

- messages [2-13](#)

- recipients [12-77](#)

- settings [2-13](#), [12-77](#)

- severities [12-77](#)

alternate MX host [11-2](#)

anonymize user names [5-3](#)

#### appliance status

- Web Security appliances [8-22](#)

archiving reports [4-77](#), [4-79](#), [5-83](#), [5-89](#)

AsyncOS reversion [12-25](#)

AsyncOS update servers [12-33](#)

AsyncOS upgrades [12-17](#)

#### automatic update

- interval [12-34](#)

automatic updates [12-34](#)

AutoSupport feature [2-14](#), [12-79](#)

---

### B

backing up [12-8](#)

#### backup

- scheduling [12-11](#)

- smaller appliance [12-36](#)

- to smaller appliance [12-36](#)

backupconfig command [12-113](#)

#### browser

- multiple windows or tabs [2-10](#)

- requirements [2-10](#)

## C

case-sensitivity  
     in LDAP queries [10-11](#)

chain query  
     creating [10-15](#)  
     LDAP [10-14](#)

Change Password link [12-66](#)

changing your password [12-66](#)

clean message [4-17](#), [4-21](#)

CLI Audit Logs [13-3](#)

Client Malware Risk  
     report [5-50](#)

comments [11-8](#)  
     comments in imported files [11-8](#)

configuration  
     overview [3-1](#)  
     publishing to Web Security appliances [8-13](#)

configuration file [12-103](#)  
     CLI [12-110](#)  
     XML [12-103](#)

Configuration Master  
     assigning Web Security appliances to [3-13](#), [8-8](#), [D-25](#)  
     configuring Web Security features [8-11](#)  
     preconfiguring [8-9](#)  
     publishing [8-13](#), [8-15](#)  
         vs. advanced file publish [8-13](#)  
     what is [8-3](#)

configuring the appliance  
     L4 Traffic Monitor [5-65](#)  
     reporting [5-1](#)  
     scheduling reports [4-75](#), [5-82](#)

custom URL categories  
     overview [5-33](#)

## D

daily magnitude [4-26](#)

default  
     DNS server [12-92](#)  
     gateway [2-15](#)  
     hostname [2-15](#)  
     IP address [2-10](#)  
     router [2-15](#)

delegating administration [12-45](#), [12-51](#)  
     See also administration, distributing [12-40](#)

delivery [11-1](#)

depth of appliance [2-4](#), [2-5](#)

dimensions of appliance [2-4](#)

disaster recovery [12-36](#)

disk quotas  
     editing [12-117](#)

DLP Incident Summary page [4-40](#)

DNS [C-2](#)  
     authoritative server [12-91](#)  
     disabling reverse DNS lookup timeout [12-93](#)  
     double lookup [4-24](#)

- priority [12-91](#)
- servers [2-15, 12-91](#)
- settings [2-15, 12-94](#)
- splitting [12-91](#)
- timeout [12-91](#)
- timeout for reverse DNS lookups [12-92](#)
- DNS cache, flushing [12-93](#)
- dnsconfig command [12-90](#)
- dnsflush command [12-93](#)
- Domain-Based Executive Summary Report [4-68](#)
- Domain Name Service
  - See DNS [2-15](#)
- Domain Redirect feature, see smtpoutes command
- domains [4-26](#)
- double-DNS verified [4-23](#)
- DTD (document type definition) [12-106](#)

## E

- edit centralized email reporting [4-4](#)
- editing disk quotas [12-117](#)
- editing DNS settings via GUI [12-94](#)
- edit packet capture [2-27](#)
- email
  - clean message [4-17, 4-21](#)
- email reporting
  - edit [4-4](#)
  - enable [4-3](#)

- groups [4-4](#)
- Email Security Appliance
  - adding as managed appliance [3-10](#)
- Email Security Monitor
  - Items Displayed menu [4-24](#)
  - Time Range menu [12-102](#)
- enable email reporting [4-3](#)
- Envelope Recipient [6-6](#)
- Envelope Sender [6-6](#)
- Ethernet interfaces [B-1](#)
- event tracking [6-7](#)
  - Currently in Outbreak Quarantine [6-7](#)
  - Delivered [6-7](#)
  - DLP Violations [6-7](#)
  - Hard Bounced [6-7](#)
  - Quarantined as Spam [6-7](#)
  - Soft Bounced [6-7](#)
  - Spam Positive [6-7](#)
  - Suspect Spam [6-7](#)
  - Virus Positive [6-7](#)
- exporting
  - reports [3-21](#)
- external authentication [10-20](#)
  - enabling LDAP [12-67](#)
  - enabling RADIUS [12-68](#)

## F

- feature keys [2-30](#)

adding (GUI) manually [2-31](#)  
 firewall [2-6](#)  
 firewall ports [C-1](#)  
 FTP [C-1](#)  
 FTP Access [A-5](#)  
 FTP Poll [13-6](#)  
 FTP Push [13-6](#)  
 FTP Server Logs [13-3](#)

---

## G

globbing [11-2](#)  
 GUI [2-17](#)  
     browser requirements [2-10](#)

---

## H

height of appliance [2-4, 2-5](#)  
 hostname, setting [12-89](#)  
 HTTP [C-1](#)  
 HTTP Logs [13-3](#)  
 HTTP proxy server [12-34](#)  
 HTTPS proxy server [12-34](#)

---

## I

IMAP authentication [7-8](#)  
 installation  
     reverting [12-25](#)

international character sets [6-6](#)  
 invalid recipient [4-16, 4-20](#)  
 IP address profile pages [4-25](#)

---

## K

keys [2-30](#)

---

## L

L4 Traffic Monitor  
     configuring [5-65](#)  
     report [5-63](#)  
 language  
     specifying a default language for Cisco  
     IronPort Spam Quarantine [7-5](#)  
 last command [12-60](#)  
 LDAP [C-2](#)  
     alias consolidation queries [10-9](#)  
     chain queries [10-14](#)  
     domain-based queries [10-12](#)  
     end-user authentication queries [10-8](#)  
     external authentication [10-20, 12-67](#)  
     failover [10-16](#)  
     LDAP server profiles [10-3](#)  
     load-balancing [10-16](#)  
     multiple servers [10-16](#)  
     overview [10-1](#)  
     testing queries [10-11](#)

- test servers [10-6](#)
- LDAPS [C-2](#)
  - Global Catalog Server [C-2](#)
- limits
  - SMTP Routes [11-4](#)
- loadconfig command [12-112](#)
- log file type [13-2](#)
- logging
  - overview [13-1](#)
  - versus reporting [13-2](#)
- logheaders command [13-43](#)
- logs
  - Cisco IronPort Spam Quarantine GUI Logs [13-3](#)
  - Cisco IronPort Spam Quarantine Logs [13-3](#)
  - Cisco IronPort Text Mail Logs [13-3](#)
  - CLI Audit Logs [13-3](#)
  - comparison [13-4](#)
  - Configuration History Logs [13-9](#)
  - definition [13-1](#)
  - extensions in filenames [13-45](#)
  - format [13-2](#)
  - FTP Server Logs [13-3](#)
  - global attributes [13-41](#)
  - HTTP Logs [13-3](#)
  - Injection Debug Logs [13-4](#)
  - levels [13-38](#)
  - log subscription defined [13-2](#)
  - message headers in [13-43](#)
  - NTP Logs [13-3](#)

- Reporting Logs [13-3](#)
- Reporting Query Logs [13-3](#)
- rolling over [13-7](#)
- Safelist/Blocklist Logs [13-4](#)
- SCP Push [13-6](#)
- SMA Logs [13-4](#)
- Status Logs [13-4](#)
- subscriptions [13-6](#)
- syslog push [13-6](#)
- log subscriptions [13-2, 13-6](#)

---

## M

- mailconfig command [12-111](#)
- mailertable feature [11-1](#)
- MAIL FROM
  - configuring for notifications [12-76](#)
- mail trend graph [4-14](#)
- mapping domains [11-2](#)
- message headers [13-43](#)
- message tracking
  - See tracking
- message variables
  - Cisco IronPort Spam Quarantine notifications [7-11](#)
- monitoring
  - scheduling reports [4-75, 5-82](#)
  - summary data [4-1, 5-1](#)
- monitoring services

enabling on Security Management Appliance [3-2](#)

Email reporting [4-12, 4-17](#)

Web reporting [5-12](#)

---

## N

netmasks, selecting [B-2](#)

Network [12-71](#)

network\_access\_list [12-70](#)

networking worksheet [2-7](#)

network owner [4-26](#)

Network Owner profile pages [4-25](#)

network time protocol

See NTP

network topology [B-5](#)

non-ascii character sets [6-6](#)

No Subject [6-10](#)

NTP [C-2](#)

logs [13-3](#)

server [12-100](#)

settings [2-14](#)

---

## O

offline command [12-3](#)

offline state [12-3](#)

on-demand reports [5-89](#)

Outgoing Destinations page [4-31](#)

Outgoing Senders page [4-33](#)

Overview page

---

## P

packet capture [2-24](#)

password command [12-97](#)

passwords

changing [12-66, 12-97](#)

physical dimensions of appliance [2-4](#)

policy groups

custom URL categories [5-33](#)

POP authentication [7-8](#)

power down [12-2](#)

print page [3-20](#)

Profile for Domain pages [4-25](#)

proxy server [12-34](#)

publishconfig command [12-112](#)

publish history

viewing [8-21](#)

publishing configurations

advanced file publish [8-14, 8-18](#)

Configuration Master [8-13, 8-15](#)

to Web Security appliances [8-13](#)

viewing history [8-21](#)

---

## Q

quarantine [7-1](#)



## queries

- chain queries [10-14](#)
- domain-based [10-12](#)
- external authentication [10-20](#)
- LDAP alias consolidation [10-9](#)
- LDAP end-user authentication [10-8](#)

---

**R**

RADIUS external authentication [12-68](#)

reboot command [12-3](#)

reconfigure [2-9](#)

recursive DNS queries [12-92](#)

recursive entries

- in SMTP Routes [11-2](#)

redirecting email [11-2](#)

remote upgrades [12-20](#)

reporting filters [3-19](#), [4-11](#), [5-11](#)

Reporting Logs [13-3](#)

Reporting Query Logs [13-3](#)

reports

- archiving [4-77](#), [4-79](#), [5-83](#), [5-89](#)
- Client Detail [5-53](#)
- Client Malware Risk [5-50](#)
- exporting data [3-21](#)
- interactive display [5-1](#)
- L4 Traffic Monitor [5-63](#)
- Malware Category [5-42](#)
- Malware Threat [5-43](#)

- on-demand [5-89](#)

- print [3-20](#)

- scheduling [4-75](#), [5-82](#)

- time range for scheduled reports [4-75](#), [5-82](#)

- uncategorized URLs [5-31](#)

- URL Categories [5-28](#)

- Web Reputation Filters [5-57](#)

resetconfig command [12-6](#)

resume command [12-6](#)

reverse DNS [6-11](#)

Reverse DNS Lookup

- disabling [12-93](#)

- timeout [12-91](#)

revert

- installation [12-25](#)

rolling over log files [13-7](#)

rollovernow command [13-45](#)

root servers (DNS) [2-15](#)

routing [11-1](#)

routing taking precedence over selected interface [B-3](#)

---

**S**

Safelist/Blocklist Logs [13-4](#)

saveconfig command [12-112](#)

SBRs score [6-11](#)

scheduling a backup [12-11](#)

- instant [12-14](#)

- interruption of backup process [12-11](#)

- periodic [12-12](#)
- scp command [A-8](#)
- SCP Push [13-6](#)
- secure copy [A-8](#)
- Security Management appliance
  - backing up [12-8](#)
  - enabling services [3-2](#)
  - Incoming Mail Graph [4-14](#)
  - Incoming Mail Summary [4-14](#)
  - Outgoing Mail Graph [4-14](#)
  - Outgoing Mail Summary [4-14](#)
  - resetting [12-6](#)
  - turning off [12-2](#)
- security services settings
  - editing [8-3](#)
- SenderBase [C-2](#)
- SenderBase reputation score [6-11](#)
- SenderBase Reputation Service [4-25](#)
- serial connection pinouts [A-9](#)
- services for interfaces [A-1](#)
- sethostname command [12-89](#)
- showconfig command [12-110](#)
- shutdown command [12-2](#)
- shutting down [12-2](#)
- SMA Logs [13-4](#)
- SMTP [C-1](#)
- SMTP Authentication [6-11](#)
- SMTP Routes [11-1](#)
  - and DNS [11-4](#)
  - deleting all [11-7](#)
  - limits [11-4](#)
  - mail delivery and splintering [11-4](#)
  - maximum [11-2](#)
  - multiple host entries [11-3](#)
  - recursive entries in [11-2](#)
  - USEDNS [11-4](#)
- spam message [4-16, 4-20](#)
- Spam Quarantine, Cisco IronPort
  - default language [7-5](#)
  - defined [7-1](#)
  - deleting all messages [7-18](#)
  - end user access without authentication [7-9](#)
  - end-user authentication queries [10-8](#)
  - GUI Logs [13-3](#)
  - Logs [13-3](#)
  - message details [7-17](#)
  - message variables [7-11](#)
  - notification [7-2](#)
  - released messages and email pipeline [7-18](#)
- SSH [C-1](#)
- start packet capture [2-25](#)
- Status Logs [13-4](#)
- stopped by content filter [4-16, 4-20, E-6](#)
- stopped by reputation filtering [4-16, 4-20](#)
- streaming upgrades [12-19](#)
- subject
  - no subject [6-10](#)
- supportrequest command [2-21](#)

suspend command [12-3](#)  
 synchronizing time [2-14](#)  
 Syslog [13-6](#)  
 system administration [12-1](#)  
 System Capacity  
     All page [4-64](#)  
     Incoming Mail page [4-57](#)  
     memory page swapping [4-63, 5-79](#)  
     Outgoing Mail page [4-60](#)  
     System Load page [4-62](#)  
     WorkQueue page [4-56](#)  
 System Capacity page  
     for ESA [4-55](#)  
 system clock [2-14](#)  
 system failure  
     disaster recovery on Security Management  
     Appliance [12-36](#)  
 System Logs [13-4](#)  
 system time  
     setting [2-14](#)

---

## T

tail command [13-46](#)  
     parameters [13-47](#)  
 Telnet [C-1](#)  
 Text Mail Logs, Cisco IronPort [13-3](#)  
 tiered reporting [4-4](#)  
 time  
     choosing a range [3-18](#)

    servers [2-14](#)  
     system [2-14](#)  
 time zone  
     setting [2-13](#)  
     specifying an offset [12-99](#)  
 time zone file  
     updating [12-101](#)  
 Time Zone page [12-98](#)  
 TLS Connections page [4-8, 4-48](#)  
 tracking  
     advanced options [6-4](#)  
     event [6-7](#)  
     message details [6-3](#)  
     result set, narrowing [6-8](#)

---

## U

uncategorized URLs  
     in reports [5-31](#)  
 update server [12-33](#)  
 Update Settings page [12-32](#)  
 updating  
     time zone files [12-101](#)  
 upgrades [C-1](#)  
     remote [12-20](#)  
     streaming [12-19](#)  
 upgrade server [12-20](#)  
 URL categories  
     uncategorized URLs [5-31](#)

URL Categories report [5-28](#)

## URL Filters

custom categories [5-33](#)

user accounts [12-55](#)

user groups [12-40](#)

user names [12-57](#)

anonymous [5-3](#)

user password length [12-58](#)

user roles [12-40](#)

custom [12-45](#)

custom, for Email [12-45](#)

custom, for Web [12-51](#)

description [12-40](#)

UTF-8 [6-6](#)

process for managing [8-1](#)

publishing configurations to [8-13](#)

viewing status [8-22](#)

Web UI session timeout [12-74](#)

weight of appliance [2-4, 2-5](#)

whoami command [12-60](#)

who command [12-60](#)

width of appliance [2-4, 2-5](#)

---

## X

XML [12-103, 12-106, 12-111](#)

---

## V

virus message [4-16, 4-20](#)

Virus Types page [4-45](#)

---

## W

### Web Reporting

Overview page [4-12, 5-12](#)

### Web Reputation Filters

configuring Access Policies [5-61](#)

report [5-57](#)

### Web Security appliance

adding as managed appliance [3-10](#)