



User Guide for AsyncOS 15.5.1 for Cisco Secure Email and Web Manager - GD (General Deployment)

First Published: 2024-04-30

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

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 NON-INFRINGEMENT 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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Introduction 1

- What's New in this Release 1
- Cisco Secure Email and Web Manager Overview 4

CHAPTER 2

Setup, Installation, and Basic Configuration 7

- Solution Deployment Overview 7
- SMA Compatibility Matrix 8
- Installation Planning 8
 - Network Planning 8
 - About Integrating a Cisco Secure Email and Web Manager Appliance with Email Security Email Gateway Appliances 9
 - Deployments with Clustered Email Gateway Appliances 9
- Preparing for Setup 9
 - Physically Setting Up and Connecting the Appliance 10
 - Determining Network and IP Address Assignments 10
 - Gathering the Setup Information 10
- Accessing the Security Management Appliance 11
 - Browser Requirements 11
 - About Accessing the Web Interfaces 12
 - Accessing the Web Interface 13
 - Accessing the Legacy Web Interface 14
 - Accessing the Command Line Interface 14
 - Supported Languages 14
 - Accessing the New Web Interface on Dark Mode 15
- Accessing the Security Management Appliance API Interface Using Swagger UI 15
- Running the System Setup Wizard 15

Before You Begin	16
Overview of the System Setup Wizard	16
Launch the System Setup Wizard	17
Review the End User License Agreement	17
Configure the System Settings	17
Configure the Network Settings	18
Review Your Configuration	18
Proceeding to the Next Steps	19
About Adding Managed Appliances	19
Editing Managed Appliance Configurations	19
Removing an Appliance from the List of Managed Appliances	20
Configuring Services on the Security Management Appliance	20
Committing and Abandoning Configuration Changes	21
<hr/>	
CHAPTER 3	Working With Reports 23
Ways to View Reporting Data	23
How the Security Management Appliance Gathers Data for Reports	24
How Reporting Data is Stored	24
About Reporting and Upgrades	25
Customizing Your View of Report Data	25
Viewing Reporting Data for an Appliance or Reporting Group	25
Choosing a Time Range for Reports	26
(Web Reports Only) Choosing Which Data to Chart	26
Customizing Tables on Report Pages	27
Custom Reports	27
Modules That Cannot Be Added to Custom Reports	28
Creating Your Custom Report Page	28
Viewing Details of Messages or Transactions Included in Reports	29
Improving Performance of Email Reports	29
Exporting Reporting and Tracking Data	31
Exporting Report Data as a Comma Separated Values (CSV) File	32
Subdomains vs. Second Level Domains in Reporting and Tracking	33
Troubleshooting All Reports	33
Unable to View Report Data on Backup Security Management Appliance	34

Reporting Is Disabled	34
Email and Web Reports	34

CHAPTER 4**Working With Reports on the New Web Interface 35**

Ways to View Reporting Data	35
How the Security Management Appliance Gathers Data for Reports	36
How Reporting Data is Stored	36
About Reporting and Upgrades	37
Using the Interactive Report Pages	37
Customizing Your View of Report Data	38
Viewing Reporting Data for an Appliance or Reporting Group	38
Choosing a Time Range for Reports	39
(Web Reports Only) Choosing Which Data to Chart	39
(Email Reports Only) Customizing Views on Report Pages	40
Customizing Tables on Report Pages	40
Using Counters to Filter Data on the Trend Graphs	41
My Favorite Reports Page	41
Modules That Cannot Be Added to the My Favorite Reports Page	42
Adding Reports on the My Favorite Reports Page	42
Viewing Details of Messages or Transactions Included in Reports	43
Improving Performance of Email Reports	43
Exporting Reporting and Tracking Data	45
Exporting Report Data as a Comma Separated Values (CSV) File	46
Troubleshooting All Reports	47
Unable to View Report Data on Backup Security Management Appliance	47
Reporting Is Disabled	47

CHAPTER 5**Using Centralized Email Security Reporting 49**

Centralized Email Reporting Overview	49
Setting Up Centralized Email Reporting	50
Enabling Centralized Email Reporting	50
Enabling Centralized Email Reporting on the Legacy Web Interface	50
Enabling Centralized Email Reporting on the New Web Interface	51
Creating Email Reporting Groups	52

Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance	52
Enabling Centralized Email Reporting on Email Security Appliances	53
Working with Email Report Data	53
Working with Email Report Data on the New Web Interface	54
Searching and the Interactive Email Report Pages	55
Understanding the Email Reporting Pages	56
Table Column Descriptions for Email Reporting Pages	60
Email Reporting Overview Page	62
How Incoming Mail Messages are Counted	63
How Email Messages Are Categorized by the Appliances	63
Categorizing Email Messages on the Overview Page	64
Incoming Mail Page	66
Views Within the Incoming Mail Page	66
Incoming Mail Details Table	68
Sender Profile Pages	68
Sender Groups Report Page	69
Sender Domain Reputation Page	70
Outgoing Destinations Page	70
Outgoing Senders Page	71
Internal Users Page	72
Internal User Details Page	73
Searching for a Specific Internal User	74
DLP Incidents	74
DLP Incidents Details Table	75
DLP Policy Detail Page	75
Message Filters	75
Geo Distribution	75
High Volume Mail	75
Content Filters Page	76
Content Filter Details Page	76
DMARC Verification	77
Macro Detection	77
External Threat Feeds Page	77
Virus Types Page	78

URL Filtering Page	79
Web Interaction Tracking Page	79
Forged Email Detection Page	80
Safe Print Page	80
Mail Policy Details Report Page	80
Advanced Phishing Protection Page	81
Advanced Phishing Protection Page on Legacy Web Interface	81
Advanced Phishing Protection Page on New Web Interface	81
Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages	82
Requirements for File Analysis Report Details	82
Identifying Files by SHA-256 Hash	84
File Reputation and File Analysis Report Pages	84
Viewing File Reputation Filtering Data in Other Reports	86
For Which Files Are Detailed File Analysis Results Visible in the Cloud?	86
Mailbox Auto Remediation	86
TLS Connections Page	87
Inbound SMTP Authentication Page	88
Rate Limits Page	88
Outbreak Filters Page	89
Reporting of Graymail	91
Reporting of Marketing Messages after Upgrade to AsyncOS 9.5	91
System Capacity Page	91
How to Interpret the Data You See on System Capacity Page	92
System Capacity – Workqueue	92
System Capacity – Incoming Mail	93
System Capacity – Outgoing Mail	93
System Capacity – System Load	93
System Capacity – All	94
Threshold Indicator in System Capacity Graphs	95
Reporting Data Availability Page	95
Understanding the Email Reporting Pages on the New Web Interface	95
Mail Flow Summary Page	100
How Incoming Mail Messages are Counted	102
How Email Messages Are Categorized by the Appliances	102

Categorizing Email Messages on the Mail Flow Summary Page 103

System Capacity Page 105

 How to Interpret the Data You See on System Capacity Page 106

 System Capacity – Workqueue 106

 System Capacity – Incoming Mail 106

 System Capacity – Outgoing Mail 107

 System Capacity – System Load 107

 System Capacity – All 108

 Threshold Indicator in System Capacity Graphs 108

Advanced Malware Protection Page 108

 Advanced Malware Protection – Summary 109

 Advanced Malware Protection – AMP Reputation 109

 Advanced Malware Protection – File Analysis 110

 Advanced Malware Protection – File Retrospection 111

 Advanced Malware Protection – Mailbox Auto Remediation 111

 Requirements for File Analysis Report Details 112

 Identifying Files by SHA-256 Hash 113

 Viewing File Reputation Filtering Data in Other Reports 114

 For Which Files Are Detailed File Analysis Results Visible in the Cloud? 114

Virus Filtering Page 114

 Virus Types Detail Table 115

Macro Detection Page 116

DMARC Verification Page 116

 Domains by DMARC Verification Details Table 117

Outbreak Filtering Page 117

URL Filtering Page 119

URL Retrospection Report page 120

Forged Email Detection Page 120

Sender Domain Reputation Page 121

External Threat Feeds Page 121

Safe Print Page 122

Advanced Phishing Protection Reports Page 122

Mail Flow Details Page 122

 Views Within the Mail Flow Details Page 124

Incoming Mails Table	125
Sender Profile Pages	127
Sender Details Table	128
Sender Groups Page	129
Outgoing Destinations Page	130
Outgoing Destinations Detail Table	131
TLS Encryption Page	132
TLS Connections Details Table	134
Inbound SMTP Authentication Page	134
Rate Limits Page	136
Connections by Country Page	137
Domain Protection Page	137
User Mail Summary	138
User Mail Flow Details Table	139
Searching for a Specific Internal User	140
DLP Incident Summary Page	140
Web Interaction Page	141
Web Interaction Tracking Details	142
Remediation Reports Page	143
Message Filters Page	145
High Volume Mail Page	145
Content Filters Page	146
Content Filter Details Page	146
Reporting Data Availability Page	146
Reporting of Graymail	146
Reporting of Marketing Messages after Upgrade to AsyncOS 9.5	147
About Scheduled and On-Demand Email Reports	147
Additional Report Types	149
Domain-Based Executive Summary Report	149
Executive Summary Report	151
Scheduled Reports Page	151
Scheduling Email Reports	152
Adding Scheduled Reports	152
Editing Scheduled Reports	153

Discontinuing Scheduled Reports	153
Generating Email Reports On Demand	153
Archived Email Reports Page	155
Viewing and Managing Archived Email Reports	155
Accessing Archived Reports	155
Deleting Archived Reports	155
Scheduling and Archiving Email Reports on the New Web Interface	156
Scheduling Email Reports on the New Web Interface	156
Adding Scheduled Reports on the New Web Interface	156
Editing Scheduled Reports on the New Web Interface	157
Discontinuing Scheduled Reports on the New Web Interface	158
Archived Email Reports Page on the New Web Interface	158
Accessing Archived Reports on the New Web Interface	158
Generating Email Reports On Demand	159
Deleting Archived Reports on the New Web Interface	160
Troubleshooting Email Reports	160
Outbreak Filters Reports Do Not Show Information Correctly	160
Message Tracking Results Do Not Match Report Results After Clicking a Link in a Report	160
Advanced Malware Protection Verdict Updates Report Results Differ	161
Issues Viewing File Analysis Report Details	161
File Analysis Report Details Are Not Available	161
Error When Viewing File Analysis Report Details	161
Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance	161
Logging of File Analysis-Related Errors	162
Total Graymail or Marketing Messages Appears To Be Incorrect	162

CHAPTER 6

Using Centralized Web Reporting and Tracking	163
Centralized Web Reporting and Tracking Overview	163
Setting Up Centralized Web Reporting and Tracking	165
Enabling Centralized Web Reporting on the Security Management Appliance	165
Enabling Centralized Web Reporting on Web Security Appliances	165
Adding the Centralized Web Reporting Service to Each Managed Web Security Appliance	165
Anonymizing User Names in Web Reports	166

Working with Web Security Reports	167
Working with Web Security Reports on the New Web Interface	167
Web Reporting Page Descriptions	168
About Time Spent	170
Web Reporting Overview	171
Users Report (Web)	172
User Details (Web Reporting)	173
User Count Report (Web)	175
Web Sites Report	175
URL Categories Report	176
Reducing Uncategorized URLs	177
URL Category Set Updates and Reports	177
Using The URL Categories Page in Conjunction with Other Reporting Pages	177
Reporting Misclassified and Uncategorized URLs	178
Application Visibility Report	178
Understanding the Difference between Application versus Application Types	178
Anti-Malware Report	180
Malware Category Report	181
Malware Threat Report	181
Malware Category Descriptions	181
Advanced Malware Protection (File Reputation and File Analysis) Reports	182
Requirements for File Analysis Report Details	183
Identifying Files by SHA-256 Hash	184
Advanced Malware Protection (File Reputation and File Analysis) Report Pages	185
Viewing File Reputation Filtering Data in Other Reports	186
For Which Files Are Detailed File Analysis Results Visible in the Cloud?	186
Client Malware Risk Report	187
Web Reputation Filters Report	188
What are Web Reputation Filters?	188
Adjusting Web Reputation Settings	189
L4 Traffic Monitor Report	189
SOCKS Proxy Report	191
Reports by User Location	191
System Capacity Page	192

- Viewing the System Capacity Report 193
- How to Interpret the Data You See on the System Capacity Page 193
- System Capacity - System Load 193
- System Capacity - Network Load 194
- Note About Proxy Buffer Memory Swapping 194
- Data Availability Page 194
- Understanding the Web Reporting Pages on the New Web Interface 195
 - About Time Spent 197
 - Overview Page 197
 - Application Visibility Page 199
 - Layer 4 Traffic Monitor Page 201
 - SOCKS Proxy Page 203
 - URL Categories Page 204
 - Reducing Uncategorized URLs 205
 - URL Category Set Updates and Reports 206
 - Using The URL Categories Page in Conjunction with Other Reporting Pages 206
 - Reporting Misclassified and Uncategorized URLs 206
 - Users Page 207
 - User Details Page (Web Reporting) 208
 - Web Sites Page 210
 - HTTPS Reports Page 211
 - Anti-Malware Page 212
 - Malware Category Report 214
 - Malware Threat Report 214
 - Malware Category Descriptions 214
 - Advanced Malware Protection Page 215
 - Advanced Malware Protection - AMP Summary 216
 - Advanced Malware Protection - File Analysis 217
 - Client Malware Risk Report 217
 - Web Reputation Filters Page 218
- About Scheduled and On-Demand Web Reports 220
- Scheduling Web Reports 221
 - Storage of Scheduled Web Reports 222
 - Adding Scheduled Web Reports 222

Editing Scheduled Web Reports	223
Deleting Scheduled Web Reports	223
Additional Extended Web Reports	223
Top URL Categories—Extended	223
Top Application Types—Extended	224
Generating Web Reports on Demand	224
Archived Web Reports Page	225
Viewing and Managing Archived Web Reports	226
Schedule and Archive Web Reports on the New Web Interface	226
Scheduling Web Reports on the New Web Interface	226
Adding Scheduled Web Reports on the New Web Interface	227
Editing Scheduled Web Reports on the New Web Interface	227
Deleting Scheduled Web Reports on the New Web Interface	228
Archiving Web Reports on the New Web Interface	228
[New Web Interface] Generating Web Reports on Demand	228
Viewing and Managing Archived Web Reports on the New Web Interface	229
Web Tracking	229
Searching for Transactions Processed by Web Proxy Services	229
Malware Category Descriptions	232
Searching for Transactions Processed by the L4 Traffic Monitor	233
Searching for Transactions Processed by the SOCKS Proxy	234
Web Tracking on the New Web Interface	234
Searching for Transactions Processed by Web Proxy Services	234
Malware Category Descriptions	237
Searching for Transactions Processed by the Layer 4 Traffic Monitor	238
Searching for Transactions Processed by the SOCKS Proxy	239
Working with Web Tracking Search Results	239
Displaying More Web Tracking Search Results	239
Understanding Web Tracking Search Results	239
Viewing Transaction Details for Web Tracking Search Results	240
About Web Tracking and Advanced Malware Protection Features	240
About Web Tracking and Upgrades	241
Troubleshooting Web Reporting and Tracking	241
Centralized Reporting Is Enabled Properly But Not Working	241

- Advanced Malware Protection Verdict Updates Report Results Differ 241
- Issues Viewing File Analysis Report Details 242
 - File Analysis Report Details Are Not Available 242
 - Error When Viewing File Analysis Report Details 242
 - Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance 242
- Expected Data Is Missing from Reporting or Tracking Results 242
- PDF Shows Only a Subset of Web Tracking Data 243
- Troubleshooting L4 Traffic Monitor Reports 243
- Exported .CSV file is Different From Web Interface Data 243
- Issues Exporting Web Tracking Search Results 243

CHAPTER 7

FIPS Management 245

- FIPS Management Overview 245
- Configuration Changes in FIPS Mode 245
- Switching the Appliance to FIPS Mode 246
- Checking FIPS Mode Compliance 247

CHAPTER 8

Tracking Messages 249

- Tracking Service Overview 249
- Setting Up Centralized Message Tracking 250
 - Enabling Centralized Email Tracking 250
 - Enabling Centralized Email Tracking on the Legacy Web Interface 251
 - Enabling Centralized Email Tracking on the New Web Interface 251
 - Configuring Centralized Message Tracking on Email Security Appliances 251
 - Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance 252
 - Managing Access to Sensitive Information 253
- Checking Message Tracking Data Availability 253
- Searching for Email Messages 253
 - Searching for Email Messages on the New Web Interface 253
 - Searching for Email Messages on the Legacy Web Interface 255
 - Remediating Messages in Mailboxes 257
 - Search and Remediate Actions on Messages in the Mailboxes 258
 - Narrowing the Result Set 259

About Message Tracking and Advanced Malware Protection Features	260
Understanding Tracking Query Results	261
Message Details	261
Verdict Chart and Last State Verdicts	262
Envelope and Header Summary	263
Sending Host Summary	263
Processing Details	263
Troubleshooting Message Tracking	264
Expected Messages Are Missing from Search Results	264
Attachments Do Not Appear in Search Results	265
Exporting Message Service	265
<hr/>	
CHAPTER 9	Spam Quarantine 267
Overview of the Spam Quarantine	267
Local Versus External Spam Quarantine	267
Setting Up the Centralized Spam Quarantine	268
Enabling and Configuring Spam Quarantine	268
Enabling and Configuring the Spam Quarantine on the Legacy Web Interface	268
Enabling and Configuring Spam Quarantine on the New Web Interface	270
Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance	272
Configuring an Outbound IP Interface on the Security Management Appliance	272
Configuring the IP Interface for Browser Access to the Spam Quarantine	273
Configuring Administrative User Access to the Spam Quarantine	274
Spam Quarantine Threshold Alert	275
Configuring Spam Quarantine Threshold Alert Settings Using CLI	275
Configuring Spam Quarantine Threshold Alert Settings Using GUI	275
Limiting Which Recipients Have Mail Quarantined	276
Spam Quarantine Language	276
Edit Spam Quarantine Page	276
Using Safelists and Blocklists to Control Email Delivery Based on Sender	276
Message Processing of Safelists and Blocklists	277
Enabling Safelists and Blocklists	277
Enabling Safelists and Blocklists on the Legacy Web Interface	278
Enabling Safelists and Blocklists on the New Web Interface	278

External Spam Quarantine and Safelist/Blocklists	279
Adding Senders and Domains to Safelists and Blocklists (Administrators)	279
Syntax for Safelists and Blocklist Entries	283
Clearing All Safelists and Blocklists	284
About End-User Access to Safelists and Blocklists	284
Adding Entries to Safelists (End Users)	284
Adding Senders to Blocklists (End Users)	285
Backing Up and Restoring the Safelist/Blocklist	285
Troubleshooting Safelists and Blocklists	286
Message from Safelisted Sender Was Not Delivered	286
Configuring Spam Management Features for End Users	287
Authentication Options for End Users Accessing Spam Management Features	287
LDAP Authentication Process	288
IMAP/POP Authentication Process	289
SAML 2.0 Authentication Process	289
Setting Up End-User Access to the Spam Quarantine via Web Browser	289
Configuring End-User Access to the Spam Quarantine	290
Determining the URL for End-User Access to the Spam Quarantine	291
Which Messages an End User Sees	291
Notifying End Users About Quarantined Messages	292
Recipient Email Mailing List Aliases and Spam Notifications	294
Testing Notifications	295
Troubleshooting Spam Notifications	295
Configuring End-User Quarantine for Shared Mailbox	296
Accessing EUQ for Shared Mailbox	296
Managing Messages in the Spam Quarantine	299
Accessing the Spam Quarantine (Administrative Users)	299
Accessing the Spam Quarantine (Administrative Users)	299
Searching for Messages in the Spam Quarantine	299
Searching Very Large Message Collections	300
Viewing Messages in the Spam Quarantine	300
Delivering Messages in the Spam Quarantine	301
Deleting Messages from the Spam Quarantine	301
Disk Space for the Spam Quarantine	301

About Disabling the External Spam Quarantine	301
Troubleshooting Spam Quarantine Features	302
<hr/>	
CHAPTER 10	Centralized Policy, Virus, and Outbreak Quarantines 303
Overview of Centralized Quarantines	303
Quarantine Types	304
Centralizing Policy, Virus, and Outbreak Quarantines	305
Enabling Centralized Policy, Virus, and Outbreak Quarantines on the Security Management Appliance	307
Enabling Centralized Policy, Virus, and Outbreak Quarantines on the New Web Interface of the Appliance	307
Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance	307
Configuring Migration of Policy, Virus, and Outbreak Quarantines	308
Designating an Alternate Appliance to Process Released Messages	310
Configuring Centralized Quarantine Access for Custom User Roles	311
Disabling Centralized Policy, Virus, and Outbreak Quarantines	311
Releasing Messages When an Email Security Appliance Is Unavailable	311
Managing Policy, Virus, and Outbreak Quarantines	311
Disk Space Allocation for Policy, Virus, and Outbreak Quarantines	312
Retention Time for Messages in Quarantines	312
Default Actions for Automatically Processed Quarantined Messages	313
Checking the Settings of System-Created Quarantines	314
Configuring Policy, Virus, and Outbreak Quarantines	314
About Editing Policy, Virus, and Outbreak Quarantine Settings	316
Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned	316
About Deleting Policy Quarantines	316
PVO Quarantine Threshold Alert	317
Configuring PVO Quarantine Threshold Alert Settings using CLI	317
Configuring PVO Quarantine Threshold Alert Settings using Web Interface	317
Monitoring Quarantine Status, Capacity, and Activity	318
Alerts About Quarantine Disk-Space Usage	320
Policy Quarantines and Logging	320
About Distributing Message Processing Tasks to Other Users	320

Which User Groups Can Access Policy, Virus, and Outbreak Quarantines	321
Working with Messages in Policy, Virus, or Outbreak Quarantines	321
Viewing Messages in Quarantines	322
Quarantined Messages and International Character Sets	322
Searching for Messages in Policy, Virus, and Outbreak Quarantines	323
Modifying Search Criteria	323
Manually Processing Messages in a Quarantine	323
Sending a Copy of the Message	324
About Moving Messages Between Policy Quarantines	324
Messages in Multiple Quarantines	325
Message Details and Viewing Message Content	325
Viewing Matched Content	326
Downloading Attachments	327
About Rescanning of Quarantined Messages	327
The Outbreak Quarantine	328
Rescanning Messages in an Outbreak Quarantine	328
Rule Summary View	328
Manage by Rule Summary Link	329
Reporting False Positives or Suspicious Messages to Cisco Systems	329
Troubleshooting Centralized Policy Quarantines	329
Administrative User Cannot Choose Quarantines in Filters and DLP Message Actions	329
Messages Released from a Centralized Outbreak Quarantine Are Not Rescanned	329
<hr/>	
CHAPTER 11	Managing Web Security Appliances 331
About Centralized Configuration Management	331
Determining the Correct Configuration Publishing Method	332
Using Configuration Masters to Centrally Manage Web Security Appliances	332
Important Notes About Using Configuration Masters	335
Determine the Configuration Master Versions to Use	335
Enabling Centralized Configuration Management on the Security Management Appliance	335
Initializing and Configuring Configuration Masters	336
Initializing Configuration Masters	336
About Associating Web Security Appliances to Configuration Masters	336
Adding Web Security Appliances and Associating Them with Configuration Master Versions	337

Associating Configuration Masters to Web Security Appliances	338
Configuring Sub Configuration Masters	338
Viewing Associated Configuration Masters in the Appliance List	339
Deleting Sub Configuration Masters	339
Selecting the Sub Configuration Master as the Active Configuration	339
Configuring Settings to Publish	340
Importing from an Existing Configuration Master	340
Importing Settings from a Web Security Appliance	341
Configuring Web Security Features Directly in Configuration Masters	341
Ensuring that Features are Enabled Consistently	343
Comparing Enabled Features	344
Enabling Features to Publish	344
Disabling Unused Configuration Masters	345
Setting Up to Use Advanced File Publishing	346
Publishing Configurations to Web Security Appliances	346
Publishing a Configuration Master	346
Before You Publish a Configuration Master	346
Publishing a Configuration Master Now	348
Publishing a Configuration Master Later	349
Publishing a Configuration Master Using the Command Line Interface	349
Publishing Configurations Using Advanced File Publishing	350
Advanced File Publish: Publish Configuration Now	350
Advanced File Publish: Publish Later	351
Viewing Status and History of Publishing Jobs	351
Viewing Publish History	352
Centralized Upgrade Management	352
Setting Up Centralized Upgrade Management for Web Security Appliances	352
Enable the Centralized Upgrade Manager	352
Adding the Centralized Upgrade Service to Each Managed Web Security Appliance	353
Selecting and Downloading WSA Upgrades	354
Using the Install Wizard	355
Viewing Web Security Appliance Status	356
Viewing a Summary of Status of Web Appliances	356
Viewing Status of Individual Web Security Appliances	356

- Web Appliance Status Details 357
- System Health Dashboard on the New Web Interface 357
- Preparing For and Managing URL Category Set Updates 358
 - Understand the Impacts of URL Category Set Updates 359
 - Ensure That You Will Receive Notifications and Alerts about URL Category Set Updates 359
 - Specify Default Settings for New and Changed Categories 359
 - When the URL Category Set is Updated, Check Your Policy and Identity/Identification Profile Settings 359
- Application Visibility and Control (AVC) Updates 360
- Updating WBRS and AVC Data using CLI 360
- Troubleshooting Configuration Management Issues 360
 - In Configuration Master Identities/Identification Profiles, Groups Are Not Available 361
 - Configuration Master Access Policies Web Reputation and Anti-Malware Settings Page Settings are Not as Expected 361
 - Troubleshooting Issues when Importing Existing Configuration for Configuration Masters 361
 - Troubleshooting Configuration Publishing Failures 362

CHAPTER 12

Monitoring System Status 363

- About Security Management Appliance Status 363
- Monitoring Service Status on the New Web Interface of the Appliance 364
- Monitoring Security Management Appliance Capacity 365
 - Monitoring the Processing Queue 365
 - Monitoring CPU Utilization 365
- Monitoring Status of Data Transfer From Managed Appliances 366
- Viewing the Configuration Status of Your Managed Appliances 367
 - Additional Status Information for Web Security Appliances 367
- Monitoring Reporting Data Availability Status 368
 - Monitoring Email Security Reporting Data Availability 368
 - Monitoring Web Security Reporting Data Availability 368
- Monitoring Email Tracking Data Status 369
- Monitoring Capacity of Managed Appliances 369
- Identifying Active TCP/IP Services 369
- Replacing a Managed Appliance During Hardware Failure 369

CHAPTER 13**Integrating With LDAP 371**

- Overview **371**
- Configuring LDAP to Work with the Spam Quarantine **371**
- Creating the LDAP Server Profile **372**
 - Testing LDAP Servers **374**
- Configuring LDAP Queries **374**
 - LDAP Query Syntax **375**
 - Tokens **375**
 - Spam Quarantine End-User Authentication Queries **375**
 - Sample Active Directory End-User Authentication Settings **376**
 - Sample OpenLDAP End-User Authentication Settings **376**
 - Spam Quarantine Alias Consolidation Queries **377**
 - Sample Active Directory Alias Consolidation Settings **377**
 - Sample OpenLDAP Alias Consolidation Settings **378**
 - Testing LDAP Queries **378**
- Domain-Based Queries **378**
 - Creating a Domain-Based Query **379**
- Chain Queries **380**
 - Creating a Chain Query **380**
- Configuring AsyncOS to Work With Multiple LDAP Servers **381**
 - Testing Servers and Queries **381**
 - Failover **382**
 - Configuring the Cisco Content Security Appliance for LDAP Failover **382**
 - Load Balancing **383**
 - Configuring the Cisco Content Security Appliance for Load Balancing **383**
- Configuring External Authentication of Administrative Users Using LDAP **384**
 - User Accounts Query for Authenticating Administrative Users **384**
 - Group Membership Queries for Authenticating Administrative Users **385**
 - Enabling External Authentication of Administrative Users **386**

CHAPTER 14**Configuring SMTP Routing 387**

- SMTP Routes Overview **387**
 - SMTP Routes, Mail Delivery, and Message Splintering **388**

SMTP Routes and Outbound SMTP Authentication 388

Routing Email for Local Domains 388

 Default SMTP Route 388

Managing SMTP Routes 389

 Defining an SMTP Route 389

 SMTP Routes Limits 389

 Adding SMTP Routes 389

 Exporting SMTP Routes 390

 Importing SMTP Routes 390

 SMTP Routes and DNS 391

CHAPTER 15

Integrating with Cisco SecureX or Cisco Threat Response 393

Integrating Your Appliance with Cisco SecureX or Cisco Threat Response 393

 How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response 394

 Prerequisites 395

 Enable the Cisco SecureX Integration on your Security Management Appliance 395

 Register Cisco SecureX or Cisco Threat Response on Your Security Management Appliance 396

 Reregistering with Cisco Cloud Service Portal 396

 Confirm Whether the Registration was Successful 397

 Enabling Cisco SecureX or Threat Response on content Security Gateway 397

 Enabling Cisco Cloud Services Portal on Content Security Gateway 398

 Performing Threat Analysis using Cisco SecureX Ribbon 398

 Accessing the Cisco SecureX Ribbon 399

 Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu 400

 Performing Remedial Actions on Messages in Cisco SecureX Threat Response 401

CHAPTER 16

Distributing Administrative Tasks 403

About Distributing Administrative Tasks 403

Assigning User Roles 403

 Predefined User Roles 404

 Custom User Roles 406

 About Custom Email User Roles 406

 About Custom Web User Roles 410

Deleting Custom User Roles	412
User Roles with Access to the CLI	412
Using LDAP	412
Access to Quarantines	412
Users Page	412
About Authenticating Administrative Users	413
Changing the Admin User's Passphrase	413
Changing the User's Passphrase After Expiry	413
Managing Locally-Defined Administrative Users	414
Adding Locally-Defined Users	414
Editing Locally-Defined Users	415
Deleting Locally-Defined Users	415
Viewing the List of Locally-Defined Users	415
Setting and Changing Passphrases	415
Setting Passphrase and Login Requirements	416
Requiring Users to Change Passphrase on Demand	420
Locking and Unlocking Local User Accounts	420
External User Authentication	421
Configuring LDAP Authentication	421
Enabling RADIUS Authentication	421
Two-Factor Authentication	424
Enabling Two-Factor Authentication	424
Disabling Two-Factor Authentication	425
Adding an Email or Web Security appliance over SSH with Pre-Shared Keys	425
Additional Controls on Access to the Security Management Appliance	426
Configuring IP-Based Network Access	426
Direct Connections	426
Connecting Through a Proxy	427
Creating the Access List	427
Configuring the Web UI Session Timeout	429
Configuring the CLI Session Timeout	430
Controlling Access to Sensitive Information in Message Tracking	430
Displaying a Message for Administrative Users	431
Enabling and Disabling Message Banners for Administrative Users	431

Viewing Administrative User Activity	431
Viewing Active Sessions Using the Web	431
Viewing Your Recent Login Attempts	432
Viewing Administrative User Activity via the Command Line Interface	432
Troubleshooting Administrative User Access	433
Error: User Has No Access Privileges Assigned	433
User Has No Active Menus	433
Externally-Authenticated Users See Preferences Option	433

CHAPTER 17
Common Administrative Tasks 435

Performing Administrative Tasks	436
Cisco Content Security Management Appliances Licensing	436
Working with Feature Keys	436
Smart Software Licensing	437
Overview	437
Enabling Smart Software Licensing	441
Registering the Appliance with Cisco Smart Software Manager	441
Obtaining and Using VLN, Certificate, and Key Details to Register Secure Email and Web Manager in Air-Gap Mode	442
Requesting for Licenses	443
Deregistering the Appliance from Smart Cisco Software Manager	444
Reregistering the Appliance with Smart Cisco Software Manager	444
Changing Transport Settings	444
Renewing Authorization and Certificate	444
Reserving Feature Licenses	445
Updating Smart Agent	449
Alerts	449
Command Line Interface	450
Smart Software Licensing Key Points for AsyncOS 14.0	468
Performing Maintenance Tasks Using CLI Commands	468
Shutting Down the Security Management Appliance	468
Rebooting the Security Management Appliance	469
Taking the Security Management Appliance Out of Service	469
CLI Examples: suspend and suspendtransfers Commands	470

Resuming from a Suspended State	470
CLI Examples: resume and resumetransfers Commands	470
Resetting the Configuration to Factory Defaults	470
Resetconfig CLI Command	471
Diagnostic - Reload Subcommand	471
Diagnostic - Reload Status Command	472
Displaying the Version Information for AsyncOS	472
Enabling Remote Power Cycling	472
Monitoring System Health Using SNMP	474
Example: snmpconfig Command	474
Backing Up Security Management Appliance Data	476
What Data Is Backed Up	476
Restrictions and Requirements for Backups	476
Backup Duration	478
Availability of Services During Backups	478
Interruption of a Backup Process	478
Prevent the Target Appliance From Pulling Data Directly from Managed Appliances	479
Receiving Alerts About Backup Status	479
Scheduling Single or Recurring Backups	479
Starting an Immediate Backup	480
Checking Backup Status	480
Backup Information in Log Files	481
Other Important Backup Tasks	481
Making a Backup Appliance the Primary Appliance	481
Disaster Recovery on the Security Management Appliance	482
Upgrading Appliance Hardware	484
Upgrading AsyncOS	484
Batch Commands for Upgrades	485
Determining Network Requirements for Upgrades and Updates	485
Choosing an Upgrade Method: Remote vs. Streaming	485
Streaming Upgrade Overview	485
Remote Upgrade Overview	486
Hardware and Software Requirements for Remote Upgrades	486
Hosting a Remote Upgrade Image	487

Important Differences in Remote Upgrading Method	487
Configuring Upgrade and Service Update Settings	487
Upgrade and Update Settings	488
Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies	489
Configuring the Update and Upgrade Settings from the GUI	491
Upgrade Notifications	492
Before You Upgrade: Important Steps	492
Upgrading AsyncOS	492
Viewing Status of, Canceling, or Deleting a Background Download	494
After Upgrading	495
About Reverting to an Earlier Version of AsyncOS	495
Important Note About Reversion Impact	495
Reverting AsyncOS	495
About Updates	497
About URL Category Set Updates for Web Usage Controls	497
Configuring the Appliance to Trust Proxy Server Communication	497
Configuring the Return Address for Generated Messages	499
Managing Alerts	499
Alert Types and Severities	500
Alert Delivery	500
Viewing Recent Alerts	501
About Duplicate Alerts	501
Cisco AutoSupport	501
Hardware Alert Descriptions	502
System Alert Descriptions	502
Changing Network Settings	506
Changing the System Hostname	506
The sethostname Command	506
Configuring Domain Name System Settings	506
Specifying DNS Servers	507
Multiple Entries and Priority	507
Using the Internet Root Servers	507
Reverse DNS Lookup Timeout	508
DNS Alert	508

Clearing the DNS Cache	508
Configuring DNS Settings via the Graphical User Interface	508
Configuring TCP/IP Traffic Routes	509
Managing Static Routes in the GUI	509
Modifying the Default Gateway (GUI)	509
Configuring the Default Gateway	509
Secure Communication Protocol	510
Specifying a Secure Communication Protocol	510
Configuring the System Time	510
Using a Network Time Protocol (NTP) Server	511
(Recommended) Setting Appliance System Time Using the Network Time Protocol (NTP)	511
Selecting a GMT Offset	512
Updating Time Zone Files	512
Automatically Updating Time Zone Files	512
Manually Updating Time Zone Files	512
Configuration File Page	513
Saving and Importing Configuration Settings	513
Managing Configuration Files	513
Saving and Exporting the Current Configuration File	514
Loading a Configuration File	514
Resetting the Current Configuration	516
Rolling Back to a Previously Committed Configuration	516
CLI Commands for Configuration Files	517
The showconfig, mailconfig, and saveconfig Commands	517
The loadconfig Command	518
The rollbackconfig Command	518
The publishconfig Command	518
The trailblazerconfig Command	518
The updatepvocert Command	519
Uploading Configuration Changes Using the CLI	520
Managing Disk Space	521
(Virtual Appliances Only) Increasing Available Disk Space	521
Viewing Disk Space, Quotas and Usage	522
About Disk Space Maximums and Allocations	522

Ensuring That You Receive Alerts About Disk Space	522
Managing Disk Space for the Miscellaneous Quota	523
Reallocating Disk Space Quotas	523
Managing Data Storage Time	524
Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances	525
SSO Using SAML 2.0	525
About SSO and SAML 2.0	525
SAML 2.0 SSO Workflow	526
Guidelines and Limitations for SAML 2.0	527
Logout	527
General	527
Spam Quarantine Access for Administrators	527
How to Configure SSO on your Cisco Security Management Appliance	527
Prerequisites	527
Configure Cisco Content Security Management Appliance as a Service Provider	528
Configuring the Identity Provider to Communicate with Cisco Security Management Appliance	530
Configure Identity Provider Settings on Cisco Content Security Management Appliance	532
Enable SAML Authentication	533
How to Configure SSO for Spam Quarantine	534
Prerequisites	534
Configure Cisco Content Security Management Appliance as a Service Provider	535
Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance	536
Configure Identity Provider Settings on Cisco Content Security Management Appliance	538
Enable SSO for Spam Quarantine	539
Configuring OpenID Connect 1.0 on Cisco Content Security Management for AsyncOS APIs	539
Overview	539
Workflow	540
Sample Access Token	540
Prerequisites	541
Configuring OpenID Connect on Appliance	541
Configuring OpenID Connect on Appliance using CLI	542
Customizing Your View	542
Using Favorite Pages	542

Setting Preferences	543
General Settings	544
Monitoring Web Usage Analytics	544
Improving Web Interface Rendering	544
Restarting and Viewing Status of Services Enabled on Appliance	544
Managing Lists of Certificate Authorities	546
Disabling the System Certificate Authority List	546
Importing a Custom Certificate Authority List	547
Exporting a Certificate Authority List	547
Displaying Trust Root Certificate	548
Deleting Custom Certificate	548
Configuring CRL Sources	548
Configuring CRL Sources using GUI	549
Configuring Global Settings for CRL Sources	550
Configuring CRL Sources using CLI	550
Receiving and Delivering Messages with Internationalised Domain Names (IDNs)	552
Prerequisites IDN	553
Features Configurable using IDN Domains in Cisco Secure Email and Web Manager	553
FQDN	554
Validation on Peer Certificate	554
Validation on Peer Certificate Using the GUI	554
Validation on Peer Certificate Using the CLI	555
Custom CA Validation	555
Appliance Certificate Validation	555
X.509 Certificate	556
Validation of Peer Certificate	556
Validation of Peer Certificate using GUI	557
Validation of Peer Certificate using CLI	557
Custom CA Certificate Validation	557
Appliance Certificate Validation	558
Single Pane of Glass	558
SPoG Add a Cisco Secure Email and Web Manager	559
SPoG Edit a Cisco Secure Email and Web Manager	560
SPoG Delete a Cisco Secure Email and Web Manager	562

SPoG Enable Services on a Cisco Secure Email and Web Manager	562
SPoG Viewing details on primary Cisco Secure Email and Web Manager	563

CHAPTER 18**Logging 565**

Logging Overview	565
Logging Versus Reporting	565
Log Retrieval	565
Filename and Directory Structure	567
Log Rollover and Transfer Schedule	567
Timestamps in Log Files	568
Logs Enabled by Default	568
Log Types	569
Summary of Log Types	569
Log Type Comparison	572
Using Configuration History Logs	574
Using CLI Audit Logs	574
Using FTP Server Logs	575
Using HTTP Logs	576
Using Spam Quarantine Logs	576
Using Spam Quarantine GUI Logs	577
Using Text Mail Logs	577
Sample Text Mail Log	578
Examples of Text Mail Log Entries	579
Generated or Rewritten Messages	582
Sending a Message to the Spam Quarantine	582
Using NTP Logs	583
Using Reporting Logs	583
Using Reporting Query Logs	584
Using Safelist/Blocklist Logs	584
Using SMA Logs	585
Using Status Logs	586
Using System Logs	588
Understanding Tracking Logs	589
Using Audit Logs	589

Log Subscriptions	591
Configuring Log Subscriptions	591
Setting the Log Level	592
Creating a Log Subscription in the GUI	593
Editing Log Subscriptions	593
Configuring Global Settings for Logging	594
Logging Message Headers	594
Configuring Global Settings for Logging by Using the GUI	595
Rolling Over Log Subscriptions	595
Rolling Over Logs in Log Subscriptions	596
Rolling Over Logs Immediately Using the GUI	596
Rolling Over Logs Immediately via the CLI	596
Viewing the Most Recent Log Entries in the GUI	596
Viewing the Most Recent Entries in Logs (tail Command)	596
Configuring Host Keys	597

CHAPTER 19
Troubleshooting 601

Collecting System Information	601
Troubleshooting Hardware Issues	601
Troubleshooting Feature Setup Issues	601
General Troubleshooting Resources	602
Troubleshooting Issues with Specific Functionality	602
Responding to Alerts	603
Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware	603
Additional Alert Descriptions	603
Working with Technical Support	603
Opening or Updating a Support Case from the Appliance	603
Getting Support for Virtual Appliances	604
Enabling Remote Access for Cisco Technical Support Personnel	604
Enabling Remote Access to Appliances With an Internet Connection	605
Enabling Remote Access to Appliances Without a Direct Internet Connection	605
Disabling a Tech Support Tunnel	606
Disabling Remote Access	606
Checking the Status of the Support Connection	606

Running a Packet Capture 606
 Remotely Resetting Appliance Power 607

APPENDIX A IP Interfaces and Accessing the Appliance 609
 IP Interfaces and Accessing the Appliance 609
 IP Interfaces 609
 Configuring IP Interfaces 610
 Creating IP Interfaces Using the GUI 610
 Accessing the Appliance via FTP 611
 Secure Copy (scp) Access 613
 Accessing via a Serial Connection 613
 Pinout Details for the Serial Port in 80- and 90- Series Hardware 614
 Pinout Details for the Serial Port in 70-Series Hardware 614

APPENDIX B Assigning Network and IP Addresses 617
 Ethernet Interfaces 617
 Selecting IP Addresses and Netmasks 617
 Sample Interface Configurations 618
 IP Addresses, Interfaces, and Routing 618
 Summary 619
 Strategies for Connecting Your Content Security Appliance 619

APPENDIX C Firewall Information 621
 Firewall Information 621

APPENDIX D Web Security Management Examples 625
 Web Security Management Examples 625
 Web Security Appliance Examples 625
 Example 1: Investigating a User 625
 Example 2: Tracking a URL 627
 Example 3: Investigating Top URL Categories Visited 627

APPENDIX E Additional Resources 629
 Cisco Notification Service 629

Documentation	629
Third Party Contributors	630
Training	630
Knowledge Base Articles (TechNotes)	631
Registering Azure Active Directory Application	631
Cisco Support Community	631
Customer Support	632
Registering for a Cisco Account	632
Cisco Welcomes Your Comments	632

APPENDIX F

End User License Agreement	633
Cisco Systems End User License Agreement	633
Supplemental End User License Agreement for Cisco Systems Content Security Software	639



CHAPTER 1

Introduction

This chapter contains the following sections:

- [What's New in this Release, on page 1](#)
- [Cisco Secure Email and Web Manager Overview, on page 4](#)

What's New in this Release

This section describes the new features and enhancements in this release of AsyncOS for Secure Email and Web Manager.

Table 1: What's New in AsyncOS 15.5.1

Feature	Description
TLS 1.3 Support for Web Interface and API Server	You can use TLS 1.3 for TLS communication across the legacy or new web interfaces of your Secure Email and Web Manager and the API services. For more information, see Secure Communication Protocol , on page 510.

Feature	Description
Monitoring Vault Service and Sending Alerts	

Feature	Description
	<p>Your Secure Email and Web Manager now monitors the Vault service and keeps track of its status, whether it is initialized or not. It also sends appropriate alert messages and logs status information into mail_logs.</p> <p>You can access the alert logs using one of the following ways:</p> <ul style="list-style-type: none"> • Navigate to System Administration > Alerts page on the web interface, and click the View Top Alerts button. • Use the <code>displayalerts</code> command in the CLI. <p>If the Vault service fails to initialize due to any issues, you receive alert messages (in the mail, on the web interface, and in the CLI) to indicate that the Vault service is down, and you have to execute the Vault Recovery process to restore the Vault service.</p> <p>Note If the upgrade fails while upgrading to AsyncOS 15.5.1, then you should check for the Vault service error in upgrade_logs. If a Vault service error is identified, then you must restore the Vault service or proceed with the upgrade process without saving the configuration.</p> <p>You will receive alert messages in the following scenarios:</p> <ul style="list-style-type: none"> • If the Vault service fails to initialize after you upgrade to AsyncOS 15.5.1, you receive alert messages through the mail, on the web interface, and in the CLI. • If any of the services of your Secure Email and Web Manager use the Vault service that fails to initialize, you receive alert messages through the mail, on the web interface, and in the CLI. If encryption is enabled, you always receive an alert mail. If encryption is disabled, you receive an alert mail only if the services using the Vault service are configured. You can check the encryption status using the <code>adminaccessconfig>encryptconfig</code> subcommand. <p>The Vault monitoring mechanism checks the Vault service every 75 minutes. If it is down, then it sends alert messages until the Vault service is restored.</p> <p>For information on an example of a successful vault health check and initialization log entry, see Successful Vault Health Check and Initialization, on page 582.</p> <p>To restore the Vault service, you have to execute the Vault Recovery process.</p> <p>Note If the encryption (CLI> <code>adminaccessconfig>encryptconfig</code>) is enabled, ensure that you always save and keep a copy of Secure Email and Web Manager's configuration to avoid data loss.</p> <p>For more information on how to save the Secure Email and Web</p>

Feature	Description
	<p>Manager's configuration, see Saving Secure Email and Web Manager's Configuration section in the Release Notes.</p> <p>For information on how to execute the Vault Recovery process, see Executing Vault Recovery Process to Resolve Vault Issues section in the Release Notes.</p>
Mandatory Usage of Cisco Smart Software Licensing for On-Premises Users	<p>The Cisco Smart Software Licensing usage is mandatory from this release (all releases post AsyncOS 15.0 release) for Cisco Secure Email and Web Manager.</p> <p>Note From this release onwards, there will be no support for classic licensing for On-Premises users. You will no longer be able to order new feature licenses or renew existing feature licenses in the Classic Licensing mode.</p> <p>Prerequisite: Make sure you create a smart account in the Cisco Smart Software Manager portal and enable Cisco Smart Software Licensing on your Secure Email and Web Manager. For more information, see Smart Software Licensing, on page 437.</p> <p>After you enable Cisco Smart Software Licensing, you can upgrade your Secure Email and Web Manager to this release and continue to use the existing feature licenses in the Smart Licensing mode.</p>
Search Filter Enhancement	<p>To enhance your search, two new filters, Contains and Does Not Contain, are added to the drop-down list on the Search ribbon at the bottom of the reporting pages on the new web interface.</p> <p>For more information, see Searching and the Interactive Email Report Pages , on page 55</p>

Cisco Secure Email and Web Manager Overview

AsyncOS for Cisco Secure Email and Web Manager incorporates the following features:

- **External 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 Policy, Virus, and Outbreak Quarantines:** Provide a single interface for managing these quarantines and the messages quarantined in them from multiple Email gateways. Allows you to store quarantined messages behind the firewall.
- **Centralized reporting:** Run reports on aggregated data from multiple Email and Web Security appliances. The same reporting features available on individual appliances are available on Secure Email and Web Manager appliances.
- **Centralized tracking:** Use a single interface to track email messages and web transactions that were processed by multiple Email and Web Security appliances.
- **Centralized Configuration Management for Web Security appliances:** For simplicity and consistency, manage policy definition and policy deployment for multiple Web Security appliances.



Note The Secure Email and Web Manager appliance is not involved in centralized email management, or ‘clustering’ of Email Gateway.

- **Centralized Upgrade Management:** You can simultaneously upgrade multiple Web Security appliances (WSAs) using a single Secure Email and Web Manager Appliance (SMA).
- **Backup of data:** Back up the data on your Secure Email and Web Manager appliance, including reporting and tracking data, quarantined messages, and lists of safe and blocked senders.
- **Support for Internationalized Domain Name (IDN):** AsyncOS 14.0 can now receive and deliver messages with email addresses that contain IDN domains. Currently, your content security gateway provides support of IDN domains for the following languages only:
 - Indian Regional Languages: Hindi, Tamil, Telugu, Kannada, Marati, Punjabi, Malayalam, Bengali, Gujarati, Urdu, Assamese, Nepali, Bangla, Bodo, Dogri, Kashmiri, Konkani, Maithili, Manipuri, Oriya, Sanskrit, Santali, Sindhi, and Tulu.
 - European and Asian Languages: French, Russian, Japanese, German, Ukrainian, Korean, Spanish, Italian, Chinese, Dutch, Thai, Arabic, and Kazakh.

For this release, you can only configure few features using IDN domains in your content security gateway.

- SMTP Routes Configuration Settings- Add or edit IDN domains, Export or import SMTP routes using IDN domains.
- Reporting Configuration Settings: View IDN data - (usernames, email addresses, and domains) in the reports.
- Message Tracking Configuration Settings: View IDN data- (usernames, email addresses, and domains) in message tracking.
- Policy, Virus, and Outbreak Quarantine Configuration Settings: View messages with IDN domains that may be transmitting malware, as determined by the anti-virus engine, View messages with IDN domains caught by Outbreak Filters as potentially being spam or malware, View messages with IDN domains caught by message filters, content filters, and DLP message actions.
- Spam Quarantine Configuration Settings- View messages with IDN domains detected as spam or suspected spam, Add email addresses with IDN domains to the safelist and blocklist categories.

You can coordinate your security operations from a single Secure Email and Web Manager appliance or spread the load across multiple appliances.



CHAPTER 2

Setup, Installation, and Basic Configuration

This chapter contains the following sections:

- [Solution Deployment Overview](#), on page 7
- [SMA Compatibility Matrix](#), on page 8
- [Installation Planning](#), on page 8
- [Preparing for Setup](#), on page 9
- [Accessing the Security Management Appliance](#), on page 11
- [Accessing the Security Management Appliance API Interface Using Swagger UI](#), on page 15
- [Running the System Setup Wizard](#), on page 15
- [About Adding Managed Appliances](#), on page 19
- [Configuring Services on the Security Management Appliance](#), on page 20
- [Committing and Abandoning Configuration Changes](#), on page 21

Solution Deployment Overview

To configure your Cisco Secure Email and Web Manager to provide service to your Cisco Security solution:

	On These Appliances	Do This	More Information
Step 1	All appliances	Ensure that your appliances meet the system requirements for the features you will use. If necessary, upgrade your appliances.	See the SMA Compatibility Matrix , on page 8.
Step 2	Secure Email gateway	Before you introduce centralized services to your environment, configure all Email Security appliances to provide the security features you want, and verify that all features are working as expected on each appliance.	See the documentation for your Cisco Email Security release.
Step 3	Web Security appliances	Before you introduce centralized services to your environment, configure at least one Web Security appliance to provide the security features you want, and verify that all features are working as expected.	See the AsyncOS for Cisco Web Security Appliances User Guide.

	On These Appliances	Do This	More Information
Step 4	Secure Email and Web Manager appliance	Set up the appliance and run the System Setup Wizard.	See the Installation Planning , on page 8, Preparing for Setup , on page 9 and the Running the System Setup Wizard , on page 15.
Step 5	All appliances	Configure each centralized service that you want to deploy.	Start with the Configuring Services on the Security Management Appliance , on page 20.

SMA Compatibility Matrix

For compatibility of your Security Management appliance with Email Security appliances and Web Security appliances, and for compatibility of configuration files when importing and publishing Web Security appliance configurations, see the Compatibility Matrix at

<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>.

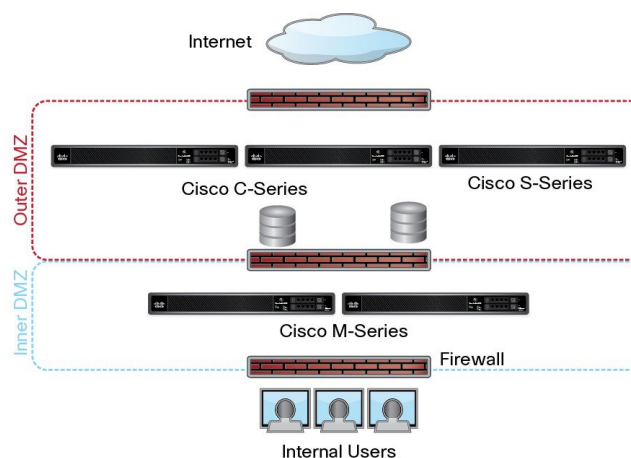
Installation Planning

- [Network Planning](#) , on page 8
- [About Integrating a Cisco Secure Email and Web Manager Appliance with Email Security Email Gateway Appliances](#) , on page 9
- [Deployments with Clustered Email Gateway Appliances](#) , on page 9

Network Planning

The Cisco Secure Email and Web Manager 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 .

Figure 1: Typical Network Configuration Incorporating the Security Management appliance



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

Corporate data centers can share a Cisco Secure Email and Web Manager 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 spam quarantine.

After you connect the Email Security appliance and the Web Security appliances to a Cisco Secure Email and Web Manager 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.

About Integrating a Cisco Secure Email and Web Manager Appliance with Email Security Email Gateway Appliances

Additional information about integrating the Cisco Secure Email and Web Manager appliance with your Email Gateway appliances, see the “Centralizing Services on a Cisco Content Security Management Appliance” chapter in the user documentation or online help for your Email Gateway appliance.

Deployments with Clustered Email Gateway Appliances

The Cisco Secure Email and Web Manager appliance cannot be placed in a cluster of Email Gateway appliances that are using the email appliances’ centralized management feature. However, clustered Email Gateway appliances can deliver messages to the Cisco Secure Email and Web Manager appliance for centralized reporting and tracking and to quarantine messages.

Preparing for Setup

Before you run the System Setup Wizard:

-
- Step 1** Review the latest release notes for your product. See [Network Planning](#) , on page 8.
 - Step 2** Verify that the components of your security solution are compatible. See the [SMA Compatibility Matrix](#), on page 8.
 - Step 3** Ensure that your network and physical space are ready to support this deployment. See [Installation Planning](#) , on page 8.
 - Step 4** Physically set up and connect the Security Management appliance. See [Physically Setting Up and Connecting the Appliance](#) , on page 10.
 - Step 5** Determine network and IP address assignments. See [Determining Network and IP Address Assignments](#), on page 10.
 - Step 6** Gather information about your system setup. See [Gathering the Setup Information](#), on page 10.
-

Physically Setting Up and Connecting the Appliance

Before you follow the procedures in this chapter, complete the steps described in the quick start guide that came with your appliance. In this guide, it is assumed that you have unpacked the appliance, physically installed it in a rack, and turned it on.

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.

Determining Network and IP Address Assignments



Note If you have already cabled your appliance to your network, ensure that the default IP address for the content security appliance does not conflict with other IP addresses on your network. The IP address that is pre-configured on the Management port of each appliance 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.

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 [Assigning Network and IP Addresses, on page 617](#).



Note If you are running a firewall on your network between the Internet and the content security appliance, it may be necessary to open specific ports for the appliance to work properly. For more information on firewalls, see [Firewall Information, on page 621](#)

Always use the same IP address on the Security Management appliance for receiving and sending email messages to the Email Security appliances. For an explanation, see information about Mail Flow in the documentation for your Email Security appliance.

Note that IPv6 is not supported for communication between the Cisco Secure Email and Web Manager appliance and the appliances it manages.

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 [Assigning Network and IP Addresses, on page 617](#) for detailed information about network and IP addresses.

The following table shows the system setup worksheet

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

Accessing the Security Management Appliance

The Security Management appliance has a standard web-based graphical user interface, a separate web-based interface for managing the spam quarantine, a command-line interface, and special or limited web interfaces for administrative users granted access to specific features and functionality.

- [Browser Requirements, on page 11](#)
- [About Accessing the Web Interfaces , on page 12](#)
- [Accessing the Legacy Web Interface, on page 14](#)
- [Accessing the Web Interface , on page 13](#)
- [Accessing the Command Line Interface, on page 14](#)
- [Supported Languages, on page 14](#)
- [Accessing the New Web Interface on Dark Mode, on page 15](#)

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).

Table 2: Supported Browsers and Releases

Browser	Windows 10 and later	MacOS 10.6 and later
Safari	—	Latest Stable Version
Google Chrome	Latest Stable Version	Latest Stable Version
Mozilla Firefox	Latest Stable Version	Latest Stable Version
Microsoft Edge	Latest Stable Version	Latest Stable Version

- Safari (Latest Stable Version)
- Firefox (Latest Stable Version)
- Google Chrome (Latest Stable Version)
- Microsoft Edge (Latest Stable Version)

Browsers are supported only for operating systems officially supported by the browser.

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.

For a seamless navigation and rendering of HTML pages, Cisco recommends using the following browsers to access the new web interface of the appliance (AsyncOS 12.0 and later):

- Google Chrome (Latest Stable Version)
- Mozilla Firefox (Latest Stable Version)

You can access the legacy web interface of the appliance on any of the supported browsers.

The supported resolution for the new web interface of the appliance (AsyncOS 12.0 and later) is between 1280x800 and 1680x1050. The best viewed resolution is 1440x900, for all the browsers.



Note Cisco does not recommend viewing the new web interface of the appliance on higher resolutions.

About Accessing the Web Interfaces

The Secure Email and Web Manager appliance has two web interfaces: the standard administrator interface, available by default on port 80, and the spam quarantine end user interface, available by default on port 82. The spam quarantine HTTPS interface defaults to port 83 when enabled.

Because you can specify HTTP or HTTPS when configuring each of the web interfaces (go to **Management Appliance > Network > IP Interfaces** on the Secure Email and Web Manager 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 spam quarantine end user web interface through HTTPS on port 83, you are asked to reauthenticate if you return to the admin web interface.



Note Do not perform any configuration changes simultaneously using:

- Multiple tabs on the same browser.
- Multiple browsers on the same system or two different systems.

Also, do not use concurrent web interface and CLI sessions as it may lead to unexpected behavior.

Accessing the Web Interface

Step 1 Open your web browser and enter the IP address or host name of your appliance.

Step 2 [New Web Interface Only] You can access the new web interface in any one of the following ways:

Note The new web interface of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the `trailblazerconfig` command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.

- When `trailblazerconfig` CLI command is enabled, use the following URL -
`https://example.com:<trailblazer-https-port>/ng-login`

where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

For more information on the `trailblazerconfig` CLI command, see [The `trailblazerconfig` Command, on page 518](#).

- When `trailblazerconfig` CLI command is disabled, use the following URL -
`https://example.com:<https-port>/ng-login`

where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

- Log in to the legacy web interface and click **Security Management appliance is getting a new look. Try it!!** link to access the new web interface.

- Important**
- Make sure that AsyncOS API is enabled on the appliance.
 - You must login to the legacy web interface of the appliance.
 - If `trailblazerconfig` is enabled, the configured HTTPS port must be opened on the firewall. The default HTTPS port is 4431.
Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.
 - If `trailblazerconfig` is disabled, the AsyncOS API ports configured in **Management Appliance > Network > IP Interfaces**, are opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443.

Step 3 Enter the following default values:

- User name: `admin`
- Passphrase: `ironport`

Note This passphrase is NOT valid after you complete the System Setup Wizard, either using the web interface or the command-line interface.

Accessing the Legacy Web Interface



Note You must login to the Security Management Appliance to access the legacy web interface. For more information, see [Accessing the Web Interface](#), on page 13

To enable and configure reporting, message tracking, quarantines, network access, and monitor system status, you must access the legacy web interface.


To access the legacy web interface from the new web interface, click on the gear icon  as shown in the following figure:

Figure 2: Accessing the Legacy Web Interface from the



The legacy web interface opens in a new browser window. You must log in again to access it.

If you want to log out of the appliance completely, you need to log out of both the new and legacy web interfaces of your appliance.

Accessing the Command Line Interface

The command line interface, or CLI, is accessed on the Email and Web Manager appliance in the same way that the CLI is accessed on all Cisco Secure Email and Web Manager appliances. There are, however, some differences:

- System setup must be performed through the GUI.
- Some CLI commands are not available on the appliance. For a list of which commands are not supported, see the IronPort AsyncOS CLI Reference Guide for Cisco Secure Email and Web Manager Appliances.

For production deployments, you should use SSH to access the CLI. Use a standard SSH client to access the appliance on port 22. For lab deployments, you can also use telnet; however, this protocol is not encrypted.

Supported 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 (traditional and simplified)
- Russian

To choose the GUI and default reporting language, do one of the following:

- Set the language preference. See [Setting Preferences](#), on page 543.
- Use the Options menu at the top right side of the GUI window to select the language for the session.

(The method that works depends on the method used to authenticate your login credentials.)

Accessing the New Web Interface on Dark Mode

Dark Mode is a reversed color scheme that utilizes light-colored typography, UI elements, and iconography on dark backgrounds. You can now use dark mode on the new web interface of your appliance.

To switch to the dark mode web interface on your appliance, click on the user information section on the top right corner of the new web interface and select **Dark Mode**.

Accessing the Security Management Appliance API Interface Using Swagger UI

Swagger UI allows you to visualize and interact with the API resources of your appliance. This is automatically generated from your API specifications. For more information, see <https://swagger.io/tools/swagger-ui/>.

You can log in to the Swagger UI on the new web interface of your Secure Email and Web Manager appliance in any one of the following ways:

- Use the following URL - `https://example.com:<trailblazer-https-port>/swagger`

where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.



Note You must enable the trailblazer HTTPS port on the appliance to access the Swagger UI. For more information on the `trailblazerconfig` CLI command, see [The trailblazerconfig Command](#), on page 518.

- Log in to the new web interface of your appliance. Click the ? button on the upper-right corner and select **API Help: Swagger** from the drop-down. The Swagger UI opens in a new browser window.

Running the System Setup Wizard

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.

The Security Management appliance supports this wizard via the GUI only. It does not support system setup through the command line interface (CLI).

- [Before You Begin](#) , on page 16
- [Overview of the System Setup Wizard](#) , on page 16

Before You Begin

Complete all tasks in the [Preparing for Setup](#) , on page 9.



Caution 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.

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



Caution 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.



Note By default, 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 passphrase. If the session times out while you are running the System Setup Wizard, you need to start over from the beginning. To change the timeout limit, see [Configuring the Web UI Session Timeout](#), on page 429.

Overview of the System Setup Wizard

Step 1 [Launch the System Setup Wizard](#) , on page 17

Step 2 [Review the End User License Agreement](#), on page 17

Step 3 [Configure the System Settings](#), on page 17

- Notification settings and AutoSupport
- System time settings
- Admin passphrase

Step 4 [Configure the Network Settings](#), on page 18

- Hostname of the appliance
- IP address, network mask, and gateway of the appliance
- Default router and DNS settings

Step 5 [Review Your Configuration](#), on page 18

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 6 [Proceeding to the Next Steps, on page 19](#)

Launch the System Setup Wizard

To launch the wizard, log in to the GUI as described in the [Accessing the Web Interface , on page 13](#). 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 (Management Appliance > System Administration > System Setup Wizard).

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.

Configure the System Settings

Entering an Email Address for System alertsAlerts

AsyncOS sends alert messages through email if there is a system error that requires your 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, on page 499](#).

Setting the Time

Set the time zone on the Security Management appliance so that timestamps in reports, 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, but Cisco recommends using an Network Time Protocol (NTP) server to synchronize time with other servers on your network or the Internet. By default, the Cisco NTP server (time.sco.cisco.com) is added as an entry to synchronize the time on your Secure Email and Web Manager 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, on page 510](#).

Setting the Passphrase

You must change the passphrase: adminpassphrase for the AsyncOS admin account. Keep the passphrase in a secure location. Changes to the passphrase take effect immediately.



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

Enabling AutoSupport

The AutoSupport feature (enabled by default) notifies Customer Support about issues with the Security Management appliance so that they can provide optimal support. For more information, see the [Cisco AutoSupport, on page 501](#).

Configure the Network Settings

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



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 deerrouter (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, on page 506](#).



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.

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.

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

If the page appears not to respond when you click **Install This Configuration**, this is because the appliance is now using the the new IP address that you specified in the wizard. To continue using the appliance, use the new IP address. If you followed the instructions in the Quick Start Guide to temporarily change the IP address of the computer you used to access your new hardware appliance, revert your computer's IP address to its original settings first.

Proceeding to the Next Steps

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.

Depending on the process you used to access the appliance in order to run the system setup wizard, the **System Setup Next Steps** page appears. If this page does not appear automatically, you can access it by choosing **Management Appliance > System Administration > Next Steps**.

Click on any of the links on the System Setup Next Steps page to proceed with the configuration of your Cisco Secure Email and Web Manager.

About Adding Managed Appliances

You will add managed Email and Web Security appliances to the Security Management appliance when you configure the first centralized service for each appliance.

Supported Email and Web Security appliances are shown in the [SMA Compatibility Matrix, on page 8](#).


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.

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

Instructions for adding managed appliances are included in the following procedures:

- [Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance](#) , on page 52
- [Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance](#) , on page 252
- [Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance](#) , on page 272
- [Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance](#), on page 307
- [Adding the Centralized Web Reporting Service to Each Managed Web Security Appliance](#) , on page 165
- [Adding Web Security Appliances and Associating Them with Configuration Master Versions](#) , on page 337

Editing Managed Appliance Configurations

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 In the Security Appliance section, click on the name of the appliance you want to edit.

Step 4 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 5 Click **Submit** to submit your changes on the page, then click Commit Changes to commit your changes.

Removing an Appliance from the List of Managed Appliances

Before you begin

You may need to disable any enabled centralized services on the remote appliance before you can remove that appliance from the Security Management appliance. For example, if the Centralized Policy, Virus, and Outbreak Quarantine service is enabled, you must disable that service first on the Email Security appliance. See the documentation for your email or web security appliance.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 In the Security Appliances section, and click the trash can icon in the row for the managed appliance that you want to delete.

Step 4 In the confirmation dialog box, click **Delete**.

Step 5 Submit and commit your changes.

Configuring Services on the Security Management Appliance

Email security services:

- [Using Centralized Email Security Reporting, on page 49](#)
- [Tracking Messages, on page 249](#)
- [Spam Quarantine, on page 267](#)
- [Centralized Policy, Virus, and Outbreak Quarantines, on page 303](#)

Web security services:

- [Centralized Policy, Virus, and Outbreak Quarantines, on page 303](#)
- [Managing Web Security Appliances, on page 331](#)

Committing and Abandoning Configuration Changes

After you make most configuration changes in the Cisco Secure Email and Web Manager GUI, you must explicitly commit the changes.

Figure 3: The Commit Changes Button



To	Do This
Commit all pending changes	Click the orange Commit Changes button at the top right side of the window. Add a description of the changes and then click commit. If you have not made any changes that require a commit, then a gray No Changes Pending button appears instead of Commit Changes.
Abandon all pending changes	Click the orange Commit Changes button at the top right side of the window, then click Abandon Changes.



Note The configuration changes made on the old web interface is updated on the new web interface, after you logout and login to the new Cisco Content Security Management web interface.

Related Topic

- [Rolling Back to a Previously Committed Configuration](#) , on page 516



CHAPTER 3

Working With Reports

This chapter contains the following sections:

- [Ways to View Reporting Data](#) , on page 23
- [How the Security Management Appliance Gathers Data for Reports](#), on page 24
- [Customizing Your View of Report Data](#) , on page 25
- [Viewing Details of Messages or Transactions Included in Reports](#) , on page 29
- [Improving Performance of Email Reports](#) , on page 29
- [Exporting Reporting and Tracking Data](#) , on page 31
- [Subdomains vs. Second Level Domains in Reporting and Tracking](#), on page 33
- [Troubleshooting All Reports](#) , on page 33
- [Email and Web Reports](#) , on page 34

Ways to View Reporting Data

Table 3: Ways To View Reporting Data

To	See
View and customize web-based interactive report pages	<ul style="list-style-type: none"> • Customizing Your View of Report Data , on page 25 • Using Centralized Email Security Reporting, on page 49 • Centralized Policy, Virus, and Outbreak Quarantines, on page 303
Automatically generate recurring PDF or CSV reports	<ul style="list-style-type: none"> • Scheduling Email Reports, on page 152 • Scheduling Web Reports , on page 221
Generate a PDF or CSV report on demand	<ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Generating Web Reports on Demand , on page 224
Export raw data as a CSV (Comma-separated values) file	<ul style="list-style-type: none"> • Exporting Reporting and Tracking Data , on page 31 • Exporting Report Data as a Comma Separated Values (CSV) File , on page 32

To	See
Generate a PDF of report data	Exporting Reporting and Tracking Data , on page 31
Email report information to yourself and other people	<ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Scheduling Email Reports, on page 152 • Generating Web Reports on Demand , on page 224 • Scheduling Web Reports , on page 221
Find information about specific transactions	Viewing Details of Messages or Transactions Included in Reports , on page 29



Note For differences between logging and reporting, see [Logging Versus Reporting](#), on page 565.

How the Security Management 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.

Reporting Data includes transactions involving both IPv4 and IPv6.



Note When gathering data for reports, the Security Management appliance applies the timestamp 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](#), on page 510.

How Reporting Data is Stored

All of the appliances store reporting data. The following table shows what time periods that each appliance stores data.

Table 4: Reporting Data Storage on the Email and Web Security Appliances

	Minute	Hourly	Daily	Weekly	Monthly	Yearly
Local Reporting on Email Security appliance or Web Security appliance	•	•	•	•	•	
Centralized Reporting on Email Security appliance or Web Security appliance	•	•	•	•		
Security Management appliance		•	•	•	•	•

About Reporting and Upgrades

New reporting features may not apply to transactions that occurred before upgrade, because the required data may not have been retained for those transactions. For possible limitations related to reporting data and upgrades, see the Release Notes for your release.

Customizing Your View of Report Data

When viewing report data in the web interface, you can customize your view.

To	Do This
View data per appliance or reporting group	Viewing Reporting Data for an Appliance or Reporting Group, on page 25
Specify a time range	Choosing a Time Range for Reports , on page 26
(For Web reports) Choose which data to chart	(Web Reports Only) Choosing Which Data to Chart , on page 26
Customize tables	See Customizing Tables on Report Pages , on page 27
Search for specific information or a subset of data to view	<ul style="list-style-type: none"> • For Email reports, Searching and the Interactive Email Report Pages , on page 55. • For Web reports, look for a Find or Filter option at the bottom of most tables. • Some tables include links (in blue text) to details for aggregated data.
Specify report-related preferences	See Setting Preferences , on page 543
Create a custom report with only the charts and tables you want	See Custom Reports , on page 27.




Note Not all customization features are available for every report.

Viewing Reporting Data for an Appliance or Reporting Group

For Mail Flow Summary and System Capacity reports for Email, you can view data from all appliances, or from any one centrally-managed appliance.

For Email reports, if you have created groups of Email Security appliances as described in [Creating Email Reporting Groups, on page 52](#), you can view the data for each reporting group.

To specify the view, select an appliance or group from the **View Data For** list on supported pages.

If you are viewing report data on the Security Management appliance to which you have recently taken backup from another Security Management appliance, you must first add (but do not establish a connection to) each appliance in  > **Management Appliance** > **Centralized Services** > **Security Appliances**.

Choosing a Time Range for Reports

Most predefined report pages allow you to choose a Time Range for the data to include. The time range that you select is used for 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:



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



Note All reports display date and time information based on the systems configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT to accommodate multiple systems in multiple time zones around the world.



Note In the new web interface, if the reporting data is already aggregated by month, you cannot select the date to view day-wise data as the day-wise data is not available after aggregation. In this case, you can select only the first day of every month, and complete reporting data for that month is displayed.



Tip You can specify a default time range that will always display each time you log in. For information, see [Setting Preferences](#), on page 543.

(Web Reports Only) Choosing Which Data to Chart

The default charts on each Web Reporting page display commonly-referenced data, but you can choose to chart different data instead. If a page has multiple charts, you can change each chart.

Generally, the chart options are the same as the columns of the table in the report. However, some columns cannot be charted.

Charts reflect all available data in a table column, regardless of the number of items (rows) you choose to display in the associated table.

Step 1 Click the **Chart Options** link below a chart.

Step 2 Choose the data to display.

Step 3 Click **Done**.

Customizing Tables on Report Pages

Table 5: Customizing Tables on Web Report Pages

To	Do This	More Information
<ul style="list-style-type: none"> Show additional columns Hide visible columns Determine available columns for a table 	Click the Columns link below the table, select the columns to display, then click Done .	For most tables, some columns are hidden by default. Each each report page offers different columns. See also Table Column Descriptions for Email Reporting Pages , on page 60.
Reorder table columns	Drag a column heading to the desired new position	—
Sort the table by the heading of your choice.	Click a column heading.	—
Display more or fewer rows of data	From the Items Displayed drop-down list at the top right of a table, choose a number of rows to display.	For Web reports, you can also set a preference for a default number of rows to display; see Setting Preferences , on page 543.
View details about a table entry, where available	Click a blue entry in the table	See also Viewing Details of Messages or Transactions Included in Reports , on page 29.
Narrow the pool of data to a specific subset	Choose or enter a value in the filter setting below the table, where available	For Web reports, available filters are discussed on each individual report page description. See Web Reporting Page Descriptions , on page 168.

Custom Reports

You can create a custom email security report page by assembling charts (graphs) and tables from existing report pages.



Note On Email Security appliances, starting in release 9.6, “My Reports” is called “My Dashboard”.

To	Do This
Add modules to your custom report page	See: <ul style="list-style-type: none"> • Modules That Cannot Be Added to Custom Reports • Creating Your Custom Report Page , on page 28
View your custom report page	<ol style="list-style-type: none"> 1. Choose Email > Reporting > My Reports. 2. Select the time range to view. The time range selected applies to all reports, including all modules on the My Reports page. <p>Newly-added modules appear at the top of the custom report.</p>
Rearrange modules on your custom report page	Drag and drop modules into the desired location.
Delete modules from your custom report page	Click the [X] in the top right corner of the module.
Generate a CSV version of your custom report	See: <ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Generating Web Reports on Demand , on page 224
Periodically generate a CSV version of your custom report	See: <ul style="list-style-type: none"> • Scheduling Email Reports, on page 152 • Scheduling Web Reports , on page 221

Modules That Cannot Be Added to Custom Reports

- All modules on the **Management Appliance > Centralized Services > System Status** page
- All modules on the **Email > Reporting > Reporting Data Availability** page
- All modules on the **Email > Message Tracking > Message Tracking Data Availability** page
- The following per-domain modules from the Sender Profile detail report page: Current Information from SenderBase, Sender Group Information, and Network Information
- The **Past Year Virus Outbreak Summary** chart and **Past Year Virus Outbreaks** table on the Outbreak Filters report page

Creating Your Custom Report Page

Before you begin

- Ensure that the modules that you want to add can be added. See [Modules That Cannot Be Added to Custom Reports](#) .
- Delete any default modules that you do not need by clicking the [X] in the top right corner of the module.

Step 1 Use one of the following methods to add a module to your custom report page:

Note Some modules are available only using one of these methods. If you cannot add a module using one method, try another method.

- Navigate to the report page under the Email tab that has the module that you want to add, then click the [+] button at the top of the module.
- Go to Email > Reporting > My Reports and click on the [+] Report Module button at the top of one of the sections, then select the report module that you want to add. You may need to click the + button in each section on the My Reports page in order to find the module that you are looking for.

You can add each module only once; if you have already added a particular module to your report, the option to add it will not be available.

Step 2 If you add a module that you have customized (for example, by adding, deleting, or reordering columns, or by displaying non-default data in the chart), customize the modules on the My Reports page.

Modules are added with default settings. Time range of the original module is not maintained.

Step 3 If you add a chart that includes a separate legend (for example, a graph from the Overview page), add the legend separately. If necessary, drag and drop it into position beside the data it describes.

Viewing Details of Messages or Transactions Included in Reports

Step 1 Click any blue number in a table on a report page.

(Not all tables have these links.)

The messages or transactions included in that number are displayed in Message Tracking or Web Tracking, respectively.

Step 2 Scroll down to see the list of messages or transactions.

What to do next

- [Tracking Messages, on page 249](#)

Improving Performance of Email Reports

If the performance of aggregated reporting decreases due to a large number of unique entries over the course of a month, use reporting filters to restrict the aggregation of data in reports that cover the previous year (Last Year reports). 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.

Exporting Reporting and Tracking Data

Table 6: Exporting Reporting and Tracking Data on the New Web Interface

To Get This	CSV	Do This	Notes
Raw data See also Exporting Report Data as a Comma Separated Values (CSV) File , on page 32	•	<ol style="list-style-type: none"> 1. Click Export link on the top of a report page. 2. Select CSV as the required format. 3. Select the required report module that you want to export and click Download. 	The CSV file contains all applicable data, including the data visible in the chart or table.
	•	<p>Create a scheduled or on-demand report. See:</p> <ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Scheduling Email Reports, on page 152 	<p>Each CSV file may contain up to 100 rows.</p> <p>If a report contains more than one table, a separate CSV file is created for each table.</p> <p>Some extended reports are not available in CSV format.</p>
A PDF of an interactive report page	•	<ol style="list-style-type: none"> 1. Click Export link on the top of a report page. 2. Select PDF as the required format. 3. Select the required report module that you want to export and click Download. 	<p>The PDF reflects the customizations that you are currently viewing.</p> <p>PDFs are formatted to be printer-friendly.</p>
A PDF of report data	•	<p>Create a scheduled or on-demand report. See:</p> <ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Scheduling Email Reports, on page 152 	-

To Get This	CSV	Do This	Notes
(Web Security) A custom subset of report data, for example data for a particular user.	•	<ol style="list-style-type: none"> 1. Select Web from the Product drop-down and choose Tracking > Web Tracking. 2. Perform a search and click the Export link or Export All link above the search results 	CSV files include all raw data matching the search criteria.
(Email Security) A custom subset of data, for example data for a particular user.	•	<ol style="list-style-type: none"> 1. Select Email from the Product drop-down and choose Tracking > Message Tracking. 2. Perform a search and click the Export link or Export All link above the search results 	<p>The Export link downloads a CSV file with the displayed search results, up to the limit you specified in your search criteria.</p> <p>The Export All link downloads a CSV file with up to 50,000 messages that match your search criteria.</p> <p>Tip: If you need to export more than 50,000 messages, perform a series of exports for a set of shorter time ranges.</p>

Exporting Report Data as a Comma Separated Values (CSV) File

You can export raw data to a comma-separated values (CSV) file, which you can access and manipulate using database applications such as Microsoft Excel. For different ways to export data, see [Exporting Reporting and Tracking Data](#), on page 31.

Because CSV exports include only raw data, exported data from a web-based report page may not include calculated data such as percentages, even if that data appears in the web-based report.

For email message tracking and reporting data, the exported CSV data will display all data in GMT regardless of what is set on the Security Management appliance. This simplifies using data independently from the appliance, particularly 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 7: 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.
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: Number of transactions detected + 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.

Subdomains vs. Second Level Domains in Reporting and Tracking

In reporting and tracking searches, second-level domains (regional domains listed at <http://george.surbl.org/two-level-tlds>) are treated differently from subdomains, even though the two domain types may appear to be the same. For example:

- Reports will not include results for a two-level domain such as co.uk , but will include results for foo.co.uk . Reports include subdomains under the main corporate domain, such as cisco.com .
- Tracking search results for the regional domain co.uk will not include domains such as foo.co.uk , while search results for cisco.com will include subdomains such as subdomain.cisco.com .

Troubleshooting All Reports

- [Unable to View Report Data on Backup Security Management Appliance , on page 34](#)
- [Reporting Is Disabled, on page 34](#)

Unable to View Report Data on Backup Security Management Appliance

Problem

You are unable to select a single Email Security appliance for which to view report data. The **View Data For** option does not appear on the reporting page.

Solution

See also [Availability of Services During Backups](#) , on page 478.

Reporting Is Disabled

Problem

Canceling a backup in progress can disable reporting.

Solution

Reporting functionality will be restored after a backup is completed.

Email and Web Reports

For information specific to Email reports, see [Using Centralized Email Security Reporting](#), on page 49.

For information specific to Web reports, see [Using Centralized Web Reporting and Tracking](#), on page 163.



CHAPTER 4

Working With Reports on the New Web Interface

This chapter contains the following sections:

- [Ways to View Reporting Data](#) , on page 35
- [How the Security Management Appliance Gathers Data for Reports](#), on page 36
- [Using the Interactive Report Pages](#), on page 37
- [Customizing Your View of Report Data](#) , on page 38
- [My Favorite Reports Page](#), on page 41
- [Viewing Details of Messages or Transactions Included in Reports](#) , on page 43
- [Improving Performance of Email Reports](#) , on page 43
- [Exporting Reporting and Tracking Data](#) , on page 45
- [Troubleshooting All Reports](#) , on page 47

Ways to View Reporting Data

The following table shows the different ways to view reporting data:

Table 8: Ways To View Reporting Data

To	See
View and customize web-based interactive report pages	<ul style="list-style-type: none">• Using the Interactive Report Pages, on page 37• Customizing Your View of Report Data , on page 38• Using Centralized Email Security Reporting, on page 49
Automatically generate recurring CSV reports	Scheduling Email Reports , on page 152
Generate a CSV report on demand	Generating Email Reports On Demand , on page 153
Export raw data as a CSV (Comma-separated values) file	Exporting Reporting and Tracking Data , on page 31 Exporting Report Data as a Comma Separated Values (CSV) File , on page 32

To	See
Email report information to yourself and other people	Scheduling Email Reports, on page 152 Generating Email Reports On Demand , on page 153
Find information about specific transactions	Viewing Details of Messages or Transactions Included in Reports , on page 29



Note For differences between logging and reporting, see [Logging Versus Reporting, on page 565](#).

How the Security Management 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.

Reporting Data includes transactions involving both IPv4 and IPv6.



Note When gathering data for reports, the Security Management appliance applies the timestamp 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, on page 510](#).

How Reporting Data is Stored

All of the appliances store reporting data. The following table shows what time periods that each appliance stores data.

Table 9: Reporting Data Storage on the Email Security Appliances

	Minute	Hourly	Daily	Weekly	Monthly	Yearly
Local Reporting on Email Security appliance	•	•	•	•	•	
Centralized Reporting on Email Security appliance	•	•	•	•		
Security Management appliance		•	•	•	•	•

About Reporting and Upgrades

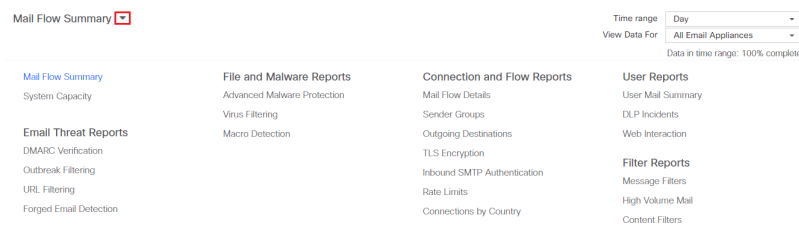
New reporting features may not apply to transactions that occurred before upgrade, because the required data may not have been retained for those transactions. For possible limitations related to reporting data and upgrades, see the Release Notes for your release.

Using the Interactive Report Pages

You can use the **Product** drop-down on the top of the web interface to switch between the Email Security appliance and Web Security appliance.

You can view the reports for the Email and Web Security appliances using the **Reports** drop-down as shown in the following figure:

Figure 4: Reports Drop-down



Note The Mail Flow Summary report page is the landing page (the page displayed after login).

You can use the **Reporting** drop-down to view your email and web reports as categorized in the following table:

Email Security Appliance	Web Security Appliance
<ul style="list-style-type: none"> • Email Threat Reports • File and Malware Reports • Connection and Flow Reports • User Reports • Filter Reports 	<ul style="list-style-type: none"> • General Reports • Threat Reports

Related Topics

- [Customizing Your View of Report Data](#) , on page 38
- [Customizing Tables on Report Pages](#) , on page 40
- [\(Web Reports Only\) Choosing Which Data to Chart](#), on page 39

Customizing Your View of Report Data

You can customize your view while viewing the report data in the web interface.

To	Do This
Specify a time range	See Choosing a Time Range for Reports , on page 26.
View data per appliance or reporting group	See Viewing Reporting Data for an Appliance or Reporting Group , on page 25
(For Web reports) Choose which data to chart	See (Web Reports Only) Choosing Which Data to Chart , on page 39
Customize tables	See Customizing Tables on Report Pages , on page 40
(Email Reports Only) Customize views	See (Email Reports Only) Customizing Views on Report Pages , on page 40
Using Counters to Filter Data on Trend Graph	See Using Counters to Filter Data on the Trend Graphs , on page 41
Specify report-related preferences	See Setting Preferences , on page 543
Search for specific information or a subset of data to view	<ul style="list-style-type: none"> • For Email reports, see Searching and the Interactive Email Report Pages , on page 55. • For Web reports, look for a Find or Filter option at the bottom of most tables. • Some tables include links (in blue text) to details for aggregated data. For more information, see Viewing Details of Messages or Transactions Included in Reports , on page 29.
Create a custom report with only the charts and tables you want	See My Favorite Reports Page , on page 41.




Note All customization features are not available for every report.

Viewing Reporting Data for an Appliance or Reporting Group

For Mail Flow Summary and System Capacity reports for Email, you can view data from all appliances, or from any one centrally-managed appliance.

For Email reports, if you have created groups of Email Security appliances as described in [Creating Email Reporting Groups](#), on page 52, you can view the data for each reporting group.

To specify the view, select an appliance or group from the **View Data For** list on supported pages.

If you are viewing report data on the Security Management appliance to which you have recently taken backup from another Security Management appliance, you must first add (but do not establish a connection to) each appliance in  > **Management Appliance** > **Centralized Services** > **Security Appliances**.

Choosing a Time Range for Reports

Most predefined report pages allow you to choose a Time Range for the data to include. The time range that you select is used for 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:



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



Note All reports display date and time information based on the systems configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT to accommodate multiple systems in multiple time zones around the world.



Note In the new web interface, if the reporting data is already aggregated by month, you cannot select the date to view day-wise data as the day-wise data is not available after aggregation. In this case, you can select only the first day of every month, and complete reporting data for that month is displayed.



Tip You can specify a default time range that will always display each time you log in. For information, see [Setting Preferences](#), on page 543.

(Web Reports Only) Choosing Which Data to Chart

The default charts on each Web Reporting page display commonly-referenced data, but you can choose to chart different data instead. If a page has multiple charts, you can change each chart.

Generally, the chart options are the same as the columns of the table in the report. However, some columns cannot be charted.

Charts reflect all available data in a table column, regardless of the number of items (rows) you choose to display in the associated table.

Step 1 Click  on a specific chart.




Step 2 Choose the required data to be displayed. The preview of the chart is displayed as per the selected options.

Step 3 Click **Apply**.

(Email Reports Only) Customizing Views on Report Pages

Most report pages allow you to choose between graphical view, tabular view or combined view. The view that you select is used to show the data on the report pages.


Table 10: Customizing Views on Email Reporting Pages

To	Do This
Show data in graph view.	Click  to view data in graphical format.
Show data in table view.	Click  to view data in tabular format.
View details about a table entry, where available	Click a blue entry in the table.
Show data in combined view.	Click  to view data in graphical and tabular format.

Customizing Tables on Report Pages

You can view, customize and sort information on the interactive tables within the report pages. The view that you select is used to show the data on the report pages.

Table 11: Customizing Tables on Report Pages

To	Do This	More Information
<ul style="list-style-type: none"> Show additional columns Hide visible columns Determine available columns for a table 	<ol style="list-style-type: none"> Click . Select the columns to display, and click Close. 	<p>For most tables, some columns are hidden by default.</p> <p>Each report page offers different columns.</p> <p>See the table column descriptions for the respective tables.</p>
Sort the table by the heading of your choice.	Click a column heading.	-
Reorder table columns	Drag a column heading to the desired new position	-
View details about a table entry, where available	Click a blue entry in the table	See also Viewing Details of Messages or Transactions Included in Reports , on page 29.

To	Do This	More Information
View details of additional rows.	You can scroll down on a table to display details of additional rows.	-
Filtering data to a specific subset	Enter a value in the filter setting below a specific table, where available	For Web reports, available filters are discussed on each individual report page description. See Understanding the Web Reporting Pages on the New Web Interface, on page 195 .

Using Counters to Filter Data on the Trend Graphs

You can filter data based on the required time range and available counters on a trend graph.


The time range that you select in the Time Range drop-down, is used for a trend graph until you select a different value.

A counters on a trend graph of the Mail Flow Summary report page is used to view data specific to different filters. Click on an available counter to filter the data.

My Favorite Reports Page

On the My Favorite Reports page, you can create a custom report page by assembling charts (graphs) and tables from all your existing email security reports.

To	Do This
Add modules to My Favorite Reports page	See: <ul style="list-style-type: none"> • Modules That Cannot Be Added to the My Favorite Reports Page, on page 42 • Adding Reports on the My Favorite Reports Page, on page 42
View My Favorite Reports page	<ol style="list-style-type: none"> 1. Select Email from the Product drop-down and choose Monitoring > My Favorite Reports from the Reports drop-down. For more information, see Using the Interactive Report Pages, on page 37. 2. Select the time range to view. The time range selected applies to all reports, including all modules on the My Favorite Reports page. <p>Newly-added modules appear at the top of the custom report.</p> <p>Note The report modules that you add on the My Favorite Reports page of the new web interface differs from the report modules added on the legacy web interface. It can also differ based on the User roles that you assign.</p>


To	Do This
Rearrange modules on the My Favorite Reports page	On the My Favorite Reports page, drag and drop the modules into the desired location.
Delete modules from the My Favorite Reports page	<p>You can delete the report modules from the My Favorite Reports page in any one of the following ways:</p> <ul style="list-style-type: none"> • Click the  in the top right corner of the required report module. • Go to the Monitoring > My Favorite Reports page and select Manage Favorites to remove the required report module.

Modules That Cannot Be Added to the My Favorite Reports Page

- All modules on the System Status page.
- All modules on the Reporting Data Availability page.
- All modules on the Message Tracking Data Availability page.
- The following per-domain modules from the Sender Profile detail report page: Current Information from SenderBase, Sender Group Information, and Network Information.
- The Past Year Virus Outbreak Summary chart and Past Year Virus Outbreaks table on the Outbreak Filters report page.


Adding Reports on the My Favorite Reports Page

Before you begin

- Ensure that the modules that you want to add can be added. See [Modules That Cannot Be Added to the My Favorite Reports Page, on page 42](#).
- Click  on the top right corner of a module to delete any default modules that you do not need.

Step 1 You can add a report module on the **My Favorite Reports** page in any one of the following ways:

Note Some modules are available only using one of these methods. If you cannot add a module using one method, try another method.

- Go to any report page under the **Reports** drop-down and click  on the top of the report module.
- From the **Reports** drop-down, choose **My Favorite Reports**, and then click **Manage Favorites**.

The report modules are listed as per the tables and charts on email report pages. Select the required report modules and click **Add** to add to the My Favorite Reports page. If you do not want any reports to be displayed on the My Favorite Report page, select the report module and click **Remove**.

You can add each module only once; if you have already added a particular module to your report, the option to add it will not be available.

Note You can add a maximum of 10 report modules on the My Favorite Reports page.

Step 2 If you add a report module that you have customized (for example, by adding, deleting, or reordering columns, or by displaying non-default data in the chart), customize the modules on the My Favorite Reports page.

Modules are added with default settings. Time range of the original module is not maintained.

Step 3 If you add a chart that includes a separate legend (for example, a graph from the Mail Flow Summary page), add the legend separately. If necessary, drag and drop it into position beside the data it describes.



Note You can export or download the **My Favorite Reports** page as a PDF. For more information, see [Exporting Reporting and Tracking Data](#).

Viewing Details of Messages or Transactions Included in Reports

Step 1 Click any blue number in a table on a report page.

(Not all tables have these links.)

The messages or transactions included in that number are displayed in Message Tracking or Web Tracking, respectively.

Step 2 Scroll down to see the list of messages or transactions.

What to do next

- [Tracking Messages, on page 249](#)

Improving Performance of Email Reports

If the performance of aggregated reporting decreases due to a large number of unique entries over the course of a month, use reporting filters to restrict the aggregation of data in reports that cover the previous year (Last Year reports). 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.

Exporting Reporting and Tracking Data

Table 12: Exporting Reporting and Tracking Data on the New Web Interface

To Get This	CSV	Do This	Notes
Raw data See also Exporting Report Data as a Comma Separated Values (CSV) File , on page 32	•	<ol style="list-style-type: none"> 1. Click Export link on the top of a report page. 2. Select CSV as the required format. 3. Select the required report module that you want to export and click Download. 	The CSV file contains all applicable data, including the data visible in the chart or table.
	•	<p>Create a scheduled or on-demand report. See:</p> <ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Scheduling Email Reports, on page 152 	<p>Each CSV file may contain up to 100 rows.</p> <p>If a report contains more than one table, a separate CSV file is created for each table.</p> <p>Some extended reports are not available in CSV format.</p>
A PDF of an interactive report page	•	<ol style="list-style-type: none"> 1. Click Export link on the top of a report page. 2. Select PDF as the required format. 3. Select the required report module that you want to export and click Download. 	<p>The PDF reflects the customizations that you are currently viewing.</p> <p>PDFs are formatted to be printer-friendly.</p>
A PDF of report data	•	<p>Create a scheduled or on-demand report. See:</p> <ul style="list-style-type: none"> • Generating Email Reports On Demand , on page 153 • Scheduling Email Reports, on page 152 	-

To Get This	CSV	Do This	Notes
(Web Security) A custom subset of report data, for example data for a particular user.	•	<ol style="list-style-type: none"> 1. Select Web from the Product drop-down and choose Tracking > Web Tracking. 2. Perform a search and click the Export link or Export All link above the search results 	CSV files include all raw data matching the search criteria.
(Email Security) A custom subset of data, for example data for a particular user.	•	<ol style="list-style-type: none"> 1. Select Email from the Product drop-down and choose Tracking > Message Tracking. 2. Perform a search and click the Export link or Export All link above the search results 	<p>The Export link downloads a CSV file with the displayed search results, up to the limit you specified in your search criteria.</p> <p>The Export All link downloads a CSV file with up to 50,000 messages that match your search criteria.</p> <p>Tip: If you need to export more than 50,000 messages, perform a series of exports for a set of shorter time ranges.</p>

Exporting Report Data as a Comma Separated Values (CSV) File

You can export raw data to a comma-separated values (CSV) file, which you can access and manipulate using database applications such as Microsoft Excel. For different ways to export data, see [Exporting Reporting and Tracking Data](#), on page 31.

Because CSV exports include only raw data, exported data from a web-based report page may not include calculated data such as percentages, even if that data appears in the web-based report.

For email message tracking and reporting data, the exported CSV data will display all data in GMT regardless of what is set on the Security Management appliance. This simplifies using data independently from the appliance, particularly 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 13: 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.
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: Number of transactions detected + 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.

Troubleshooting All Reports

- [Unable to View Report Data on Backup Security Management Appliance](#) , on page 34
- [Reporting Is Disabled](#), on page 34

Unable to View Report Data on Backup Security Management Appliance

Problem

You are unable to select a single Email Security appliance for which to view report data. The **View Data For** option does not appear on the reporting page.

Solution

See also [Availability of Services During Backups](#) , on page 478.

Reporting Is Disabled

Problem

Canceling a backup in progress can disable reporting.

Solution

Reporting functionality will be restored after a backup is completed.



CHAPTER 5

Using Centralized Email Security Reporting

This chapter contains the following sections:

- [Centralized Email Reporting Overview, on page 49](#)
- [Setting Up Centralized Email Reporting, on page 50](#)
- [Working with Email Report Data , on page 53](#)
- [Working with Email Report Data on the New Web Interface, on page 54](#)
- [Searching and the Interactive Email Report Pages , on page 55](#)
- [Understanding the Email Reporting Pages, on page 56](#)
- [Understanding the Email Reporting Pages on the New Web Interface, on page 95](#)
- [About Scheduled and On-Demand Email Reports , on page 147](#)
- [Scheduled Reports Page , on page 151](#)
- [Scheduling Email Reports, on page 152](#)
- [Generating Email Reports On Demand , on page 153](#)
- [Archived Email Reports Page , on page 155](#)
- [Viewing and Managing Archived Email Reports , on page 155](#)
- [Scheduling and Archiving Email Reports on the New Web Interface, on page 156](#)
- [Troubleshooting Email Reports , on page 160](#)

Centralized Email Reporting Overview

Your Cisco Secure Email and Web Manager appliance shows aggregated 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.

This feature centralizes the reports listed under the Monitor menu of the Email Security appliance.

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.



Note 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.

For more information about availability of report data during and after the transition to centralized reporting, see the “Centralized Reporting Mode” section of the documentation or online help for your Email Security appliance.

Setting Up Centralized Email Reporting

To set up centralized email reporting, complete the following procedures in order:

1. [Enabling Centralized Email Reporting, on page 50](#)
2. [Only for Legacy Web Interface] [Creating Email Reporting Groups, on page 52.](#)
3. [Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance , on page 52](#)
4. [Enabling Centralized Email Reporting on Email Security Appliances , on page 53](#)



Note If reporting and tracking are not consistently and simultaneously enabled and functioning properly, or are not consistently and simultaneously either centralized or stored locally on each Email Security appliance, then the message tracking results when drilling down from reports will not match expected results. This is because the data for each feature (reporting, tracking) is captured only while that feature is enabled.

Enabling Centralized Email Reporting

- [Enabling Centralized Email Reporting on the Legacy Web Interface, on page 50](#)
- [Enabling Centralized Email Reporting on the New Web Interface](#)

Enabling Centralized Email Reporting on the Legacy Web Interface

Before you begin

- All Email Security appliances should be configured and working as expected before you enable centralized reporting.
- Before enabling centralized email reporting, ensure that sufficient disk space is allocated to that service. See the [Managing Disk Space , on page 521.](#)

Step 1 Choose **Management Appliance > Centralized Services > Email > Centralized Reporting.**

Step 2 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**.

Step 4 Submit and commit your changes.

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 Space](#), on page 521 section, for more information.

What to do next

[Creating Email Reporting Groups, on page 52](#)

Enabling Centralized Email Reporting on the New Web Interface

Before you begin

- All Email Security appliances should be configured and working as expected before you enable centralized reporting.
- Before enabling centralized email reporting, ensure that sufficient disk space is allocated to that service. See the [Managing Disk Space](#), on page 521.

Step 1 On the Security Management appliance, click **Service Status** and hover over the  icon corresponding to **Reporting** card.

Step 2 Click **Edit Settings**.

Step 3 If you are enabling centralized email reporting for the first time after running the System Setup Wizard, review and accept the license agreement, and click **Proceed**.

Step 4 Click the toggle switch to enable Centralized Email Reporting.

Step 5 Create Email Reporting Groups:

- a) Click + icon to add a group.
- b) Enter an 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.

- c) Click **Add** to add the appliances to the Group Members list.

Step 6 Click **Submit**.

What to do next

For more information on managing reporting groups, see [Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance](#) , on page 52.

Creating Email Reporting Groups

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

A group can include one or more appliances, and an appliance may belong to more than one group.

Before you begin

Note This section is applicable only for Legacy Web Interface.

Make sure centralized reporting is enabled for each appliance. See [Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance](#) , on page 52.

Step 1 Choose **Management Appliance > Centralized Services > Centralized Reporting**.

Step 2 Click **Add 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 Submit and commit your changes.

What to do next

[Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance](#) , on page 52

Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance

The steps you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** If you have already added the Email Security appliance to the list on this page:
- Click the name of an Email Security appliance.
 - Select the **Centralized Reporting** service.
- Step 4** If you have not yet added Email Security appliances:
- Click Add Email Appliance.
 - In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Security Management appliance.
- Note** If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.
- The Centralized Reporting service is pre-selected.
 - Click **Establish Connection**.
 - Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.
- 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.
- Wait for the Success message to appear above the table on the page.
 - Click **Test Connection**.
 - Read test results above the table.
- Step 5** Click **Submit**.
- Step 6** Repeat this procedure for each Email Security appliance for which you want to enable Centralized Reporting.
- Step 7** Commit your changes.
-

What to do next

[Enabling Centralized Email Reporting on Email Security Appliances](#) , on page 53

Enabling Centralized Email Reporting on Email Security Appliances

You must enable centralized email reporting on each managed Email Security appliance.

For instructions, see the “Configuring an Email Security Appliance to Use Centralized Reporting” section of the documentation or online help for your Email Security appliance.

Working with Email Report Data

- For options for accessing and viewing report data, see [Ways to View Reporting Data](#) , on page 23.
- To customize your view of report data, see [Customizing Your View of Report Data](#) , on page 25

- To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#) , on page 55.
- To print or export report information, see [Exporting Reporting and Tracking Data](#) , on page 31
- To understand the various interactive report pages, see [Understanding the Email Reporting Pages](#), on page 56.
- To generate a report on demand, see [Generating Email Reports On Demand](#) , on page 153.
- To schedule reports to run automatically at intervals and times that you specify, see [Scheduling Email Reports](#), on page 152.
- To view archived on-demand and scheduled reports, see [Viewing and Managing Archived Email Reports](#) , on page 155.
- For background information, [How the Security Management Appliance Gathers Data for Reports](#), on page 24.
- To improve performance when working with large amounts of data, see [Improving Performance of Email Reports](#) , on page 29.
- To get details about an entity or number that appears as a blue link in a chart or table, click the entity or number.

For example, if your permissions allow you to do so, you can use this feature to view details about messages that violate Content Filtering or Data Loss Prevention policies. This performs the relevant search in Message Tracking. Scroll down to view results.

Working with Email Report Data on the New Web Interface

- For options for accessing and viewing report data, see [Ways to View Reporting Data](#) , on page 35.
- To customize your view of report data, see [Customizing Your View of Report Data](#) , on page 38.
- To print or export report information, see [Exporting Reporting and Tracking Data](#) , on page 31.
- To understand the various interactive report pages, see [Using the Interactive Report Pages](#), on page 37.
- To generate a report on demand, see [Generating Email Reports On Demand](#) , on page 153.
- To schedule reports to run automatically at intervals and times that you specify, see [Scheduling Email Reports](#), on page 152.
- To view archived on-demand and scheduled reports, see [Viewing and Managing Archived Email Reports](#) , on page 155.
- For background information, [How the Security Management Appliance Gathers Data for Reports](#), on page 24.
- To improve performance when working with large amounts of data, see [Improving Performance of Email Reports](#) , on page 29.
- To get details about an entity or number that appears as a blue link in a chart or table, click the entity or number.

For example, if your permissions allow you to do so, you can use this feature to view details about messages that violate Content Filtering or Data Loss Prevention policies. This performs the relevant search in Message Tracking. Scroll down to view results.

Searching and the Interactive Email Report Pages

Many of the interactive email reporting pages include a ‘**Search For:**’ drop-down menu at the bottom of the page.

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
- SHA-256
- Batch ID
- Incoming URL
- Outgoing URL
- URL Retrospection Report

On the legacy web interface, for most searches, you can choose any one of the following options:

- **Exact Match:** Search for items that exactly match the search text.
- **Starts With:** Search for items that start with the entered text (for example, starts with “ex” will match “example.com”).

On the new web interface, for most searches, you can choose any one of the following options:

- **Exact Match:** Search for items that exactly match the search text.
- **Starts With:** Search for items that start with the entered text (for example, starts with “ex” will match “example.com”).
- **Contains:** Search for items that contain the entered text.
- **Does not Contain:** Search for items that do not contain the entered text.

For IPv4 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).

For IPv6 searches, you can enter addresses using the formats in the following examples:

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

Understanding the Email Reporting Pages



Note This list represents the reports available in the latest supported release of AsyncOS for Email Security appliances. If your Email Security appliances are running earlier releases of AsyncOS, not all of these reports are available.

Table 14: Email Reporting Tab Options

Email Reporting Menu	Action
Email Reporting Overview Page	The Overview page provides a synopsis of the activity on your Email Security appliances. It includes graphs and summary tables for the incoming and outgoing messages. For more information, see the Email Reporting Overview Page, on page 62 .
Incoming Mail Page	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. For more information, see the Incoming Mail Page, on page 66 .
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. For more information, see the Sender Groups Report Page, on page 69 .
Sender Domain Reputation Page	You can use this report page to view incoming messages based on the verdict received and threat category from the SDR service For more information, see the Sender Domain Reputation Page, on page 70 .

Email Reporting Menu	Action
Outgoing Destinations Page	<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 Outgoing Destinations Page, on page 70.</p>
Outgoing Senders Page	<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 Outgoing Senders Page, on page 71.</p>
Internal Users Page	<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 Internal Users Page, on page 72.</p>
DLP Incidents	<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 DLP Incidents , on page 74.</p>
Message Filters	<p>The Message Filters page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages.</p> <p>For more information, see the Message Filters , on page 75</p>
Geo Distribution	<p>The Geo Distribution page shows the:</p> <ul style="list-style-type: none"> • Top incoming mail connections based on country of origin in graphical format. • Total incoming mail connections based on country of origin in tabular format. <p>For more information, see the Geo Distribution, on page 75.</p>
High Volume Mail	<p>The High Volume Mail page identifies attacks involving a large number of messages from a single sender, or with identical subjects, within a moving one-hour period.</p> <p>For more information, see the High Volume Mail , on page 75.</p>
Content Filters Page	<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 Content Filters Page, on page 76.</p>

Email Reporting Menu	Action
DMARC Verification	<p>The DMARC Verification page shows the top sender domains that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification, and a summary of the actions taken for incoming messages from each domain.</p> <p>For more information, see the DMARC Verification , on page 77.</p>
Macro Detection	<p>The Macro Detection Report page shows the top incoming and outgoing macro-enabled attachments by file type detected by the content or message filters.</p> <p>For more information, see the Macro Detection, on page 77</p>
External Threat Feeds Page	<p>The External Threat Feeds page shows the following reports:</p> <ul style="list-style-type: none"> • Top ETF sources that is used to detect threats in messages. • Top IOCs that matched threats detected in messages. • Top ETF sources that is used to filter malicious incoming mail connections <p>For more information, see the External Threat Feeds Page, on page 77.</p>
Virus Types Page	<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 Virus Types Page, on page 78.</p>
URL Filtering Page	<p>Use this page to view the URL categories most frequently occurring in messages, the most common URLs in spam messages, and the number of malicious and neutral URLs seen in messages.</p> <p>For more information, see the URL Filtering Page , on page 79.</p>
Web Interaction Tracking Page	<p>Identifies the end users who clicked URLs rewritten by policy or Outbreak Filter, and the action associated with each user click.</p> <p>For more information, see the Web Interaction Tracking Page, on page 79.</p>
Forged Email Detection Page	<p>The Forged Email Detection page includes the following reports:</p> <ul style="list-style-type: none"> • Top Forged Email Detection. Displays the top ten users in the content dictionary that matched the forged From: header in the incoming messages. • Forged Email Detection: Details. Displays a list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched. <p>See Forged Email Detection Page, on page 80.</p>

Email Reporting Menu	Action
Safe Print	<p>You can use the Safe Print report page to view:</p> <ul style="list-style-type: none"> • Number of safe-printed attachments based on the file type in graphical format. • Summary of safe-printed attachments based on the file type in tabular format. <p>For more information, see the Safe Print Page , on page 80.</p>
Advanced Phishing Protection Page	<p>You can use the Advanced Phishing Protection report page to view:</p> <ul style="list-style-type: none"> • Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service. • Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service. <p>For more information, see the Advanced Phishing Protection Page on Legacy Web Interface, on page 81.</p>
Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages	<p>There are three reporting pages showing file reputation and analysis data.</p> <p>For more information, see the Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages , on page 82.</p>
Mailbox Auto Remediation	<p>Use this page to view the details of the mailbox remediation results.</p> <p>See Mailbox Auto Remediation, on page 86</p>
TLS Connections Page	<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 TLS Connections Page, on page 87.</p>
Inbound SMTP Authentication Page	<p>The Inbound SMTP authentication page shows the use of client certificates and the SMTP AUTH command to authenticate SMTP sessions between the Email Security appliance and users' mail clients.</p> <p>For more information, see Inbound SMTP Authentication Page, on page 88.</p>
Outbreak Filters Page	<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 Outbreak Filters Page, on page 89.</p>
Rate Limits Page	<p>The Rate Limits page shows the mail senders (based on MAIL-FROM address) who exceed the threshold you set for the number of message recipients per sender.</p> <p>For more information, see the Rate Limits Page , on page 88.</p>

Email Reporting Menu	Action
System Capacity Page	Allows you to view the overall workload that is sending reporting data to the Security Management appliance. For more information, see the System Capacity Page, on page 91 .
Reporting Data Availability Page	Allows you to get a glimpse of the impact of the reporting data on the Security Management appliance for each appliance. For more information, see the Reporting Data Availability Page, on page 95 .
Scheduling Email Reports	Allows you to schedule reports for a specified time range. For more information, see the Scheduling Email Reports, on page 152 .
Viewing and Managing Archived Email Reports	Allows you to view and manage archived reports. For more information, see the Viewing and Managing Archived Email Reports , on page 155 . Also allows you to generate on-demand reports. See Generating Email Reports On Demand , on page 153 .

Table Column Descriptions for Email Reporting Pages

Table 15: Table Column Descriptions for Email Reporting Pages

Column Name	
Incoming Mail Details	
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 IP 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 IP Reputation Filtering.

Column Name	
Stopped by IP Reputation Filtering	<p>The value for Stopped by IP Reputation Filtering is calculated based on several factors:</p> <ul style="list-style-type: none"> • Number of “throttled” messages from this sender • Number of rejected or TCP refused connections (may be a partial count) • A conservative multiplier for the number of messages per connection <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>Note The Stopped by IP 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>
Stopped as Invalid Recipients	All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.
Stopped by Domain Reputation Filtering	The total count of messages blocked based on the reputation verdict of the sender domain.
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)
Marketing	Number of messages detected as unwanted marketing messages.
Clean	<p>All clean messages.</p> <p>Messages processed on appliances on which the graymail feature is not enabled are counted as clean.</p>
User Mail Flow Details (Internal Users Page)	
Incoming Spam Detected	All incoming spam that is detected
Incoming Virus Detected	The incoming virus that has been detected.

Column Name	
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.
Incoming and Outgoing TLS Connections: TLS Connections Page	
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.
Outbreak Filters	
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.

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.

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 The Domain-Based Executive Summary Report and the Executive Summary report are based on the [Email Reporting Overview Page, on page 62](#). For more information, see the [Domain-Based Executive Summary Report, on page 149](#) and [Executive Summary Report, on page 151](#)

Table 16: Details on the Email Reporting Overview Page

Section	Description
Time Range	A drop-down list with options for choosing a time range to view. For more information, see the Choosing a Time Range for Reports, on page 26 .
View Data for	Choose an Email Security appliance for which you want to view Overview data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .

How Incoming Mail Messages are Counted

Counts of incoming messages are 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 sender 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 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 precedence of the various filters and scanning activities greatly impacts the results of message processing.

In the example above, the various verdicts follow these rules of precedence:

- 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.

Alternately, if the message were quarantined by Outbreak Filters, it would not be counted until it was released from the quarantine and again processed through the work queue.

For complete information about message processing precedence, see chapter about the email pipeline in the online help or user guide for your Email Security appliance.

Categorizing Email Messages on the Overview Page

Messages reported in the Incoming Mail Summary on the Overview report page are categorized as follows:

Table 17: Email Categories on Overview Page

Category	Description
Stopped by IP Reputation Filtering	<p>All connections blocked by HAT policies multiplied by a fixed multiplier (see the How Incoming Mail Messages are Counted, on page 63) plus all recipients blocked by recipient throttling.</p> <p>The value for Stopped by IP Reputation Filtering is calculated based on several factors:</p> <ul style="list-style-type: none"> • Number of “throttled” messages from this sender • Number of rejected or TCP refused connections (may be a partial count) • A conservative multiplier for the number of messages per connection <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>The Stopped by IP 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>
Invalid Recipients	All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.
Stopped by Domain Reputation Filtering	The total count of messages blocked based on the reputation verdict of the sender domain.
Spam Messages Detected	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.
Virus Messages Detected	<p>The total count and percentage of messages detected as virus positive and not also spam.</p> <p>The following messages are counted in the “Virus Detected” category:</p> <ul style="list-style-type: none"> • Messages with a virus scan result of “Repaired” or “Infectious” • Messages with a virus scan result of “Encrypted” when the option to count encrypted messages as containing viruses is selected • Messages with a virus scan result of “Unscannable” when the action for unscannable messages is NOT “Deliver” • Messages with a virus scan result of “Unscannable” or “Encrypted” when the option to deliver to an alternate mail host or an alternate recipient is selected • Messages that are deleted from the Outbreak quarantine, either manually or by timing out.
Detected by Advanced Malware Protection	A message attachment was found to be malicious by file reputation filtering. This value does not include verdict updates or files found to be malicious by file analysis.
Messages with Malicious URLs	One or more URLs in the message were found to be malicious by URL filtering.

Category	Description
Stopped by Content Filter	The total count of messages that were stopped by a content filter. If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.
Stopped by DMARC	The total count of messages that failed DMARC verification.
S/MIME Verification/Decryption Failed	The total count of messages that failed S/MIME verification, decryption, or both.
Marketing Messages	The total count of advertising messages sent by recognized professional marketing groups, for example Amazon.com. This list item appears on the page only if marketing data are present in the system. This number includes marketing messages identified both by Email Security appliances on which the graymail feature is enabled and by appliances on which Marketing Email Scanning under anti-spam settings is enabled.
Social Networking Messages	The total count of notification messages from social networks, dating websites, forums, and so on. Examples include LinkedIn and CNET forums. This information is determined by the graymail feature.
Bulk Messages	The total count of advertising messages sent by unrecognized marketing groups, for example, TechTarget, a technology media company. This information is determined by the graymail feature.
Graymail Messages	This number includes marketing messages detected by the graymail feature, plus social networking messages and bulk mail. It does not include marketing messages identified on appliances on which the graymail feature is not enabled, even if those totals are included in the Marketing Messages value. Click on the number corresponding to any of the graymail categories to view a list of messages belonging to that category using Message Tracking. See also Reporting of Graymail , on page 91.
S/MIME Verification/Decryption Successful	The total count of messages that were successfully verified, decrypted, or decrypted and verified using S/MIME.
Clean Messages Accepted	This category is mail that is accepted and 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. 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. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.

Category	Description
Total Attempted Messages	This number includes spam, marketing messages (whether found by the graymail feature or by Marketing Email Scanning functionality in the anti-spam feature), social networking messages, bulk mail, and clean messages.



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.

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 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. See [Searching and the Interactive Email Report Pages](#), on page 55.
- 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](#), on page 69 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 (sender 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 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 SenderBase Reputation Service, including a sender's SenderBase Reputation Score (SBRS) 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 Sender's 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, on page 68](#).



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.

To access the mail flow information by sender group, click the **Sender Groups Report** link at the bottom of the Incoming Mail page. See [Sender Profile Pages, on page 68](#).

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, on page 56](#).

The **Email > Reporting > Incoming Mail** page offers the following views: **IP Addresses, Domains, or Network Owners**

See the [Incoming Mail Details Table, on page 68](#) for an explanation of the data included in the Incoming Mail Details interactive table.

From the **Incoming Mail** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages, on page 56](#).



Note You can generate a scheduled report for the Incoming Mail report page. See the [Scheduling Email Reports, on page 152](#).

"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 documentation or online help for your Email Security appliance.

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 Reports](#), on page 26.

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 documentation or online help for your Email Security appliance.

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 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](#), on page 68.

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](#), on page 69.

If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.

Sender Profile Pages

When you click a sender in the Incoming Mail interactive table, on the **Mail Flow Details** [New Web Interface] or **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 Mail Flow Details 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.

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.

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 documentation or online help for your Email Security appliance.

To view the Sender Groups report page, select **Email > Reporting > Sender Groups**.

From the **Sender Group Report** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages, on page 56](#).



Note You can generate a scheduled report for the Sender Group report page. See the [Scheduling Email Reports, on page 152](#).

Sender Domain Reputation Page

You can use the Sender Domain Reputation report page to view:

- Incoming messages based on the verdict received from the SDR service in graphical format.
- Summary of incoming messages based on the threat category and verdict received from the SDR service in tabular format.
- Incoming messages based on the threat category received from the SDR service in graphical format.



Note Only the messages whose SDR verdict is 'untrusted' or 'questionable' are classified under the SDR threat category, such as, 'spam,' 'malicious,' etc.

- Summary of incoming messages based on the threat category received from the SDR service in tabular format.

In the Summary of Incoming Messages handled by SDR section, you can click on the number of messages corresponding to a particular verdict to view the related messages in Message Tracking.

Outgoing Destinations Page

The **Email > Reporting > 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, malware or stopped by a content filter?
- How many messages are delivered and how many messages are hard-bounced by the destination servers?

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

Table 18: Details on the Email Reporting Outgoing Destinations 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 Choosing a Time Range for Reports, on page 26 .

Section	Description
Top Destination by Total Threat	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.
Top Destination by Clean Messages	The top destination domains of clean outgoing messages sent by your organization.
Outgoing Destination Details	<p>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 , hard-bounced messages etc.</p> <p>Note Only the following bounce types are included while counting the hard-bounced messages:</p> <ul style="list-style-type: none"> • FiveXX hard bounce • Filter hard bounce • Other hard bounce • DNS hard bounce • Expired hard bounce <p>If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.</p>

From the **Outgoing Destinations** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages, on page 56](#).



Note You can generate a scheduled report for the Outgoing Destinations page. See the [Scheduling Email Reports, on page 152](#).

Outgoing Senders Page

The **Email > Reporting > 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-positive, or spam-positive or malware 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 Senders** page, perform the following:

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 19: Details on the Email Reporting Outgoing Sender 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 Choosing a Time Range for Reports , on page 26.
Top Senders by Total Threat Messages	The top senders (by IP address or domain) of outgoing threat messages (spam, antivirus, etc.) in your organization.
Top Sender by Clean Messages	The top senders (by IP address or domain) of clean outgoing messages sent in your organization.
Sender Details	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. If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the DLP and Content Filter violations in this report, click a blue number link in the table.



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 generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages](#), on page 56.



Note You can generate a scheduled report for the **Outgoing Senders** page. See the [Scheduling Email Reports](#), on page 152.

Internal Users Page

The **Email > Reporting > 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 is sending the most external email?
- Who receives the most clean email?
- Who receives the largest number of graymail messages?
- Who receives the most spam?

- Who is triggering which content filters?
- Whose email is getting caught by content filters?

Table 20: Details on the Email Reporting Internal 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 Choosing a Time Range for Reports , on page 26.
Top Users by Clean Incoming Messages	The top users by (by IP address or domain) of clean incoming messages sent in your organization.
Top Users by Clean Outgoing Messages	The top users (by IP address or domain) of clean outgoing messages sent in your organization.
User Mail Flow Details	<p>The User Mail Flow Details interactive section breaks down the mail received and sent by each email address. You can sort the listing by clicking the column headers.</p> <p>To view details for a user, click the user name in the Internal User column. For more information, see the Internal User Details Page, on page 73.</p> <p>If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.</p>

From the **Internal Users** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages](#), on page 56.



Note You can generate a scheduled report for the Internal Users page. See the [Scheduling Email Reports](#), on page 152.

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 (such as spam detected, virus detected, detected by Advanced Malware Protection, stopped by content filter, etc.). 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](#), on page 76). 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 User Mail Summary page and the User Mail Flow Details 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”).

DLP Incidents

The **Email > Reporting > DLP Incidents (DLP Incident Summary)** page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The Email Security 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?

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

Table 21: Details on the Email Reporting DLP Incident Summary 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 Choosing a Time Range for Reports , on page 26.
Top Incidents by Severity	The top DLP incidents listed by severity.
Incident Summary	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 DLP Incident Summary page. Click the name of a DLP policy to view more detailed information.
Top DLP Policy Matches	The top DLP Policies that have been matched.
DLP Incident Details	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. For more information on the DLP Incidents Details table, see the DLP Incidents Details Table , on page 75.

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 table, click the name of the DLP Policy and the DLP Policy Page appears. For more information, see [DLP Policy Detail Page, on page 75](#).

If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

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 on the incident detail page opens up the Internal Users page. See the [Internal Users Page, on page 72](#) for more information.

Message Filters

The Message Filters page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages.

Geo Distribution

You can use the Geo Distribution report page to view:

- Top incoming mail connections based on country of origin in graphical format.
- Total incoming mail connections based on country of origin in tabular format.

The following are the scenarios when no country information is displayed for the top and total incoming mail connections:

- The sender IP address belongs to a private IP address
- The sender IP address does not get a valid SBRS.

High Volume Mail

Use reports on this page to:

- Identify attacks involving a large number of messages from a single sender, or with identical subjects, within a moving one-hour period.

- Monitor top domains to ensure that such attacks do not originate in your own domain. If this situation occurs, one or more accounts in your organization may be compromised.
- Help identify false positives so you can adjust your filters accordingly.

Reports on this page show data only from message filters that use the Header Repeats rule and that pass the number-of-messages threshold that you set in that rule. When combined with other rules, the Header Repeats rule is evaluated last, and is not evaluated at all if the message disposition is determined by a preceding condition. Similarly, messages caught by Rate Limiting never reach Header Repeats message filters. Therefore, some messages that might otherwise be considered high-volume mail may not be included in these reports. If you have configured your filters to include certain messages in the allowed list, those messages are also excluded from these reports.

For more information about message filters and the Header Repeats rule, see the online help or user guide for your Email Security appliance.

Related Topics

- [Rate Limits Page](#) , on page 88

Content Filters Page

The **Email > Reporting > 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 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, on page 76](#).

If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

From the **Content Filters** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages, on page 56](#).



Note You can generate a scheduled report for the Content Filter page. See the [Scheduling Email Reports, on page 152](#).

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, on page 73](#).

If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

DMARC Verification

The DMARC Verification page shows the top sender domains that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification, and a summary of the actions taken for incoming messages from each domain. You can use this report to fine-tune your DMARC settings and answer these kinds of questions:

- Which domains sent the most messages that failed DMARC verification?
- For each domain, what actions were taken on messages that failed DMARC verification?

For more information about DMARC verification, see the Email Authentication chapter in the online help or user guide for your Email Security appliance.

Macro Detection

You can use the Macro Detection report page to view:

- Top Incoming Macro-Enabled Attachments by File Type in graphical and tabular format.
- Top Outgoing Macro-Enabled Attachments by File Type in graphical and tabular format.

You can click on the number of macro-enabled attachments to view the related messages in Message Tracking.



Note During report generation:

- If one or more macros are detected within an archive file, the Archive Files file type is incremented by one. The number of macro-enabled attachments within an archive file are not counted.
 - If one or more macros are detected within an embedded file, the parent file type is incremented by one. The number of macro-enabled attachments within an embedded file are not counted.
-

External Threat Feeds Page

You can use the External Threat Feeds report page to view:

- Top ETF sources used to detect threats in messages in graphical format
- Summary of ETF sources used to detect threats in messages in tabular format.
- Top IOCs that matched threats detected in messages in graphical format.
- Top ETF sources used to filter malicious incoming mail connections in graphical format.
- Summary of ETF sources used to filter malicious incoming mail connections in tabular format.

In the ‘Summary of External Threat Feed Sources’ section:

- You can click on the number of messages for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular threat feed source to view the distribution of the ETF source based on the IOCs.

In the ‘Summary of Indicator of Compromise (IOC) Matches’ section:

- You can click on the number of IOCs for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular IOC to view the distribution of the IOC based on the ETF sources.

Virus Types Page

The **Email > Reporting > 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.

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.

Table 22: Details on the Email Reporting Virus Types 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 Choosing a Time Range for Reports , on page 26.
Top Incoming Virus Types Detected	This section displays a chart view of the viruses that have been sent to your network.
Top Outgoing Virus Types Detected	This section displays a chart view of the viruses that have been sent from your network.
Virus Types Detail	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 generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the [Understanding the Email Reporting Pages](#), on page 56.



Note You can generate a scheduled report for the **Virus Types** page. See the [Scheduling Email Reports](#), on page 152.

URL Filtering Page

- URL Filtering report modules are populated only if URL filtering is enabled.
- URL Filtering reports are available for incoming and outgoing messages.
- Only messages that are scanned by the URL filtering engine (either as part of anti-spam/outbreak filter scanning or through message/content filters) are included in these modules. However, not all of the results are necessarily specifically attributable to the URL Filtering feature.
- The Top URL Categories module includes all categories found in messages that have been scanned, whether or not they match a content or message filter.
- Each message can be associated with only one reputation level. For messages with multiple URLs, the statistics reflect the lowest reputation of any URL in the message.
- URLs in the global allowed list configured at Security Services > URL Filtering are not included in reports.

URLs in allowed lists used in individual filters are included in reports.

- Malicious URLs are URLs that Outbreak Filters have determined to have poor reputation. Neutral URLs are those that Outbreak Filters have determined to require click-time protection. Neutral URLs have therefore been rewritten to redirect them to the Cisco Web Security proxy.
- Results of URL category-based filters are reflected in content and message filter reports.
- Results of click-time URL evaluations by the Cisco Web Security proxy are not reflected in reports.

Web Interaction Tracking Page

- Web Interaction Tracking report modules are populated only if the Web Interaction Tracking feature is enabled on managed Email Security appliances.
- Web Interaction Tracking reports are available for incoming and outgoing messages.
- Only rewritten URLs (either by policy or Outbreak Filter) clicked by the end users are included in these modules.
- Web Interaction Tracking page includes the following reports:

Top Rewritten Malicious URLs clicked by End Users. Click on a URL to view a detailed report that contains the following information:

- A list of end users who clicked on the rewritten malicious URL.
- Date and time at which the URL was clicked.
- Whether the URL was rewritten by a policy or an outbreak filter.
- Action taken (allow, block, or unknown) when the rewritten URL was clicked. Note that, if a URL was rewritten by outbreak filter and the final verdict is unavailable, the status is shown as unknown.



Note Due to a limitation, status of all outbreak rewritten URLs are shown as unknown.

Top End Users who clicked on Rewritten Malicious URLs

Tracking Web Interaction Details. Includes the following information:

- A list of all the rewritten URLs (malicious and unmalicious). Click on a URL to view a detailed report.
- Action taken (allow, block, or unknown) when a rewritten URL was clicked.

If the verdict of a URL (clean or malicious) was unknown at the time when the end user clicked it, the status is shown as unknown. This could be because the URL was under further scrutiny or the web server was down or not reachable at the time of the user click.

- The number of times end users clicked on a rewritten URL. Click a number to view a list of all messages that contain the clicked URL.
- Note the following:
 - If you have configured a content or message filter to deliver messages after rewriting malicious URLs and notify another user (for example, an administrator), the web interaction tracking data for the original recipient is incremented if the notified user clicks on the rewritten URLs.
 - If you are sending a copy of quarantined messages containing rewritten URLs to a user other than the original recipient (for example, to an administrator) using the web interface, the web interaction tracking data for the original recipient is incremented if the other user clicks on the rewritten URLs.

Forged Email Detection Page

- The Forged Email Detection page includes the following reports:
 - **Top Forged Email Detection.** Displays the top ten users in the content dictionary that matched the forged From: header in the incoming messages.
 - **Forged Email Detection Details.** Displays a list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched.
- The Forged Email Detection reports are populated only if you are using the Forged Email Detection content filter or the forged-email-detection message filter.

Safe Print Page

You can use the Safe Print Action report page to view:

- Number of safe-printed attachments based on the file type in graphical format.
- Summary of safe-printed attachments based on the file type in tabular format.

In the ‘Summary of Safe Print File Types’ section, click the total number of safe-printed attachments to view the message details in Message Tracking.

Mail Policy Details Report Page

You can use the Mail Policy Details report page to view:

- Top incoming messages that matched a configured mail policy in graphical and tabular format.
- Top outgoing messages that matched a configured mail policy in graphical and tabular format.

In the ‘Incoming Policies’ section, click the total number of incoming messages that matched a specific mail policy to view the message details in Message Tracking.

In the ‘Outgoing Policies’ section, click the total number of incoming messages that matched a specific mail policy to view the message details in Message Tracking.

Advanced Phishing Protection Page

- [Advanced Phishing Protection Page on Legacy Web Interface, on page 81](#)
- [Advanced Phishing Protection Page on New Web Interface, on page 81](#)

Advanced Phishing Protection Page on Legacy Web Interface

The **Email > Reporting > Advanced Phishing Protection** report page displays the following:

- Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service.
- Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service.



Note If the forwarding of message metadata has failed, you must validate the configurations of the Advanced Phishing Protection feature. For more information, see the "Integrating Cisco Email Security Gateway with the Cisco Advanced Phishing Protection" chapter of the *User Guide for AsyncOS for Cisco Email Security Appliances*.

You can use the Advanced Phishing Protection report page to view:

- Total number of messages attempted to be forwarded to the Cisco Advanced Phishing Protection cloud service, in a graphical format.
- Summary of messages forwarded to the Cisco Advanced Phishing Protection cloud service in a graphical format.

Advanced Phishing Protection Page on New Web Interface

The **Monitoring > Advanced Phishing Protection** report page displays the following:

- Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service.
- Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service.



Note If the forwarding of message metadata has failed, you must validate the configurations of the Advanced Phishing Protection feature. For more information, see the "Integrating Cisco Email Security Gateway with the Cisco Advanced Phishing Protection" chapter of the *User Guide for AsyncOS for Cisco Email Security Appliances*.

You can use the Advanced Phishing Protection report page to view:

- Total number of messages attempted to be forwarded to the Cisco Advanced Phishing Protection cloud service, in a graphical format.

Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages

- [Requirements for File Analysis Report Details](#) , on page 82
- [Identifying Files by SHA-256 Hash](#) , on page 84
- [File Reputation and File Analysis Report Pages](#), on page 84
- [Viewing File Reputation Filtering Data in Other Reports](#) , on page 86

Requirements for File Analysis Report Details

- [\(Cloud File Analysis\) Ensure That the Management Appliance Can Reach the File Analysis Server](#) , on page 82
- [\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#) , on page 82
- [\(On-Premises File Analysis\) Activate the File Analysis Account](#) , on page 83
- [Additional Requirements](#) , on page 83

(Cloud File Analysis) Ensure That the Management Appliance Can Reach the File Analysis Server

In order to obtain File Analysis report details, the appliance must be able to connect to the File Analysis server over port 443. See details in [Firewall Information](#), on page 621

(Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results

In order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization, you need to join all appliances to the same appliance group.



Note If you load a license keys file that does not contain the 'cloud admin feature' key in the on-premises virtual email gateway, you can still perform auto-registration of Threat Group File Analysis using the Smart License Account ID.

-
- Step 1** In the Legacy Web Interface, click **Management Appliance > Centralized Services > Security Appliances** and scroll down to the File Analysis section.
- Step 2** If your managed appliances are pointed at different File Analysis cloud servers, select the File Analysis server from which to display result details.
- Result details will not be available for files processed by any other cloud server.
- Step 3** [Applicable if Smart Licensing is disabled on Cisco Secure Email and Web Manager] Enter the group name for file analysis reporting in the **Group Name** field and click **Group Now**.

Or

[Applicable if Smart Licensing is enabled on Cisco Secure Email and Web Manager] The system automatically registers the Smart Account ID as the group ID and displays it in the **Group Name** field.

Step 4 Configure the same group ID on each managed appliance that will share data with this appliance.

Notes:

- You can modify the group name at any time. Edit the name and click **Group Now**. This change takes effect immediately; it does not require a Commit.
- This group name is case-sensitive. This value must be identical on all appliances that will share data about files that are uploaded for analysis.
- It is suggested to use your CCOID for this value.
- An appliance can belong to only one group.
- You can add a machine to a group at any time, but you can add it only once.
- If Smart Licensing is enabled, the appliances are grouped using the Smart Account ID.

What to do next

Related Topics

[For Which Files Are Detailed File Analysis Results Visible in the Cloud? , on page 86](#)

(On-Premises File Analysis) Activate the File Analysis Account

If you have deployed an on-premises (private cloud) Cisco AMP Threat Grid Appliance, you must activate the File Analysis account for your Cisco Content Security Management appliance in order to view report details available on the Threat Grid appliance. You generally only need to do this once.

Before you begin

Ensure that you are receiving System alerts at Critical level.

Step 1 The first time you attempt to access File Analysis report details from the Threat Grid appliance, wait a few minutes and you will receive an alert that includes a link.

If you do not receive this alert, go to **Management Appliance > System Administration > Alerts** and click **View Top Alerts**.

Step 2 Click the link in the alert message.

Step 3 Activate your management appliance account.

Additional Requirements

For any additional requirements, see the Release Notes for your Security Management appliance release, available from <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format).

File Reputation and File Analysis Report Pages

Report	Description
Advanced Malware Protection	<p>Shows file-based threats that were identified by the file reputation service.</p> <p>For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.</p> <p>If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.</p> <p>Note From AsyncOS 9.6.5 onwards, Advanced Malware Protection report has been enhanced to display additional fields, graphs, and so on. The report displayed after the upgrade does not include the reporting data prior to the upgrade. To view the Advanced Malware Protection report prior to AsyncOS 9.6.5 upgrade, click on the hyperlink at the bottom of the page.</p> <p>The Incoming Malware Files by Category section shows the following:</p> <ul style="list-style-type: none"> • The percentage of blocked listed file SHAs received from the AMP reputation server that are categorized as Malware. • The percentage of blocked listed file SHAs received from the AMP for Endpoints console that are categorised as Custom Detection. <p>The threat name of a blocked listed file SHA obtained from AMP for Endpoints console is displayed as Simple Custom Detection in the Incoming Malware Threat Files section of the report.</p> <ul style="list-style-type: none"> • The percentage of blocked listed file SHAs received from the AMP for Endpoints console that are categorised as Custom Threshold. <p>You can click on the link in the More Details section of the report to view the file trajectory details of a blocked listed file SHA in the AMP for Endpoints console</p> <p>You can view the Low Risk verdict details in the Incoming Files Handed by AMP section of the report.</p>

Report	Description
Advanced Malware Protection File Analysis	<p>Displays the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.</p> <p>To view more than 1000 File Analysis results, export the data as a .csv file.</p> <p>For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are included in the allowed lists on the AMP Threat Grid appliance show as "clean." For information about allowed list, see the AMP Threat Grid documentation or online help.</p> <p>Drill down to view detailed analysis results, including the threat characteristics for each file.</p> <p>You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file.</p> <p>To view details on the server that analyzed a file, see Requirements for File Analysis Report Details , on page 82.</p> <p>If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.</p> <p>Note From AsyncOS 9.6.5 onwards, File Analysis report has been enhanced to display additional fields, graphs, and so on. The report displayed after the upgrade does not include the reporting data prior to the upgrade. To view the File Analysis report prior to AsyncOS 9.6.5 upgrade, click on the hyperlink at the bottom of the page.</p>
Advanced Malware Protection Verdict Updates	<p>Because Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data provides more information.</p> <p>The AMP Verdict Updates report lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about this situation, see the documentation for your Email Security appliance.</p> <p>To view more than 1000 verdict updates, export the data as a .csv file.</p> <p>In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.</p> <p>To view all affected messages for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click a SHA-256 link.</p>

Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A Detected by Advanced Malware Protection column may be hidden by default in applicable reports. To display additional columns, click the Columns link at the bottom of the table.

For Which Files Are Detailed File Analysis Results Visible in the Cloud?

If you have deployed public-cloud File Analysis, you can view detailed results for all files uploaded from any managed appliance that has been added to the appliance group for File Analysis.

If you have added your management appliances to the group, you can view the list of managed appliances in the group by clicking the **View Appliances in Group** button on the **Management Appliance > Centralized Services > Security Appliances > File Analysis** page.

Appliances in the analysis group are identified by the File Analysis Client ID. To determine this identifier for a particular appliance, look in the following location:

Appliance	Location of File Analysis Client ID
Email Security appliance	Advanced Settings for File Analysis section on the Security Services > File Reputation and Analysis page.
Web Security appliance	Advanced Settings for File Analysis section on the Security Services > Anti-Malware and Reputation page.
Cisco Content Security Management appliance	At the bottom of the Management Appliance > Centralized Services > Security Appliances page.

Related Topics

- [\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#), on page 82

Mailbox Auto Remediation

You can view the details of the mailbox remediation results using the Mailbox Auto Remediation report page. Use this report to view details such as:

- A list of recipients for whom the mailbox remediation was successful or unsuccessful
- Remedial actions taken on messages
- The filenames associated with a SHA-256 hash

The **Recipients for whom remediation was unsuccessful** field is updated in the following scenarios:

- The recipient is not a valid Office 365 user or the recipient does not belong to the Office 365 domain account configured on your appliance.
- The message containing the attachment is no longer available in the mailbox, for example, the end user deleted the message.
- There was a connectivity issue between your appliance and Office 365 services when the appliance was trying to perform the configured remedial action.

Click on a SHA-256 hash to view the related messages in Message Tracking.



Note After upgrading to AsyncOS 13.6.1, the message tracking status of the messages received before the upgrade remains as "Delivered" than "Remediated."

TLS Connections Page

The **Email > Reporting > 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?

Table 23: Details on the Email Reporting TLS Connections 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 Choosing a Time Range for Reports , on page 26.
Incoming TLS Connections Graph	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.
Incoming TLS Connections Summary	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.
Incoming TLS Message Summary	This table displays a summary of the total volume of incoming messages.
Incoming TLS Connections Details	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.
Outgoing TLS Connections Graph	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.
Outgoing TLS Connections Summary	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.
Outgoing TLS Message Summary	This table shows the total volume of outgoing messages

Section	Description
Outgoing TLS Connections Details	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.

Inbound SMTP Authentication Page

The Inbound SMTP Authentication page shows the use of client certificates and the SMTP AUTH command to authenticate SMTP sessions between the Email Security appliance and users' mail clients. If the appliance accepts the certificate or SMTP AUTH command, it will establish a TLS connection to the mail client, which the client will use to send a message. Since it is not possible for the appliance to track these attempts on a per-user basis, the report shows details on SMTP authentication based on the domain name and domain IP address.

Use this report to determine the following information:

- Overall, how many incoming connection use SMTP authentication?
- How many connections use a client certificated?
- How many connections use SMTP AUTH?
- What domains are failing to connect when attempting to use SMTP authentication?
- How many connections are successfully using the fall-back when SMTP authentication fails?

The Inbound SMTP Authentication page includes a graph for received connections, a graph for mail recipients who attempted an SMTP authentication connection, and a table with details on the attempts to authenticate connections.

The Received Connections graph shows the incoming connections from mail clients that attempt to authentication their connections using SMTP authentication over the time range you specify. The graph displays the total number of connections the appliance received, the number that did not attempt to authenticate using SMTP authentication, the number that failed and succeeded to authenticate the connection using a client certificate, and the number that failed and succeeded to authenticate using the SMTP AUTH command.

The Received Recipients graph displays the number of recipients whose mail clients attempted to authenticate their connections to the Email Security appliances to send messages using SMTP authentication. The graph also show the number of recipients whose connections were authenticated and the number of recipients whose connections were not authenticated.

The SMTP Authentication details table displays details for the domains whose users attempt to authenticate their connections to the Email Security appliance to send messages. For each domain, you can view the number of connection attempts using a client certificate that were successful or failed, the number of connection attempts using the SMTP AUTH command that were successful or failed, and the number that fell back to the SMTP AUTH after their client certificate connection attempt failed. You can use the links at the top of the page to display this information by domain name or domain IP address.

Rate Limits Page

Rate Limiting by envelope sender allows you to limit the number of email message recipients per time interval from an individual sender, based on the mail-from address. The Rate Limits report shows you the senders who most egregiously exceed this limit.

Use this report to help you identify the following:

- Compromised user accounts that might be used to send spam in bulk.
- Out-of-control applications in your organization that use email for notifications, alerts, automated statements, etc.
- Sources of heavy email activity in your organization, for internal billing or resource-management purposes.
- Sources of large-volume inbound email traffic that might not otherwise be considered spam.

Note that other reports that include statistics for internal senders (such as Internal Users or Outgoing Senders) measure only the number of messages sent; they do not identify senders of a few messages to a large number of recipients.

The Top Offenders by Incident chart shows the envelope senders who most frequently attempted to send messages to more recipients than the configured limit. Each attempt is one incident. This chart aggregates incident counts from all listeners.

The Top Offenders by Rejected Recipients chart shows the envelope senders who sent messages to the largest number of recipients above the configured limit. This chart aggregates recipient counts from all listeners.

Rate Limiting settings, including “Rate Limit for Envelope Senders” settings, are configured on the Email Security appliance in Mail Policies > Mail Flow Policies. For more information on rate limiting, see the documentation or online help for your Email Security appliance.

Related Topics

- [High Volume Mail](#) , on page 75

Outbreak Filters Page

The **Email > Reporting > 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?
- How long do messages stay in the Outbreak Quarantine?
- Which potentially malicious URLs are most frequently seen?

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 appliance. Local outbreak data does not include non-viral threats. Global outbreak data represents all outbreaks detected by the 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 Threat Operations Center and the release of an anti-virus signature by a major vendor. Note that not every global outbreak affects your 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 choose whether to view global or local outbreaks.

The First Seen Globally time is determined by the Threat Operations Center, based on data from the 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 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.

Other modules on this page provide:

- The number of incoming messages processed by Outbreak Filters in the selected time period.

Non-viral threats include phishing emails, scams, and malware distribution using links to an external website.

- Severity of threats caught by Outbreak Filters.

Level 5 threats are severe in scope or impact, while Level 1 represents low threat risk. For descriptions of threat levels, see the online help or user guide for your Email Security appliance.

- Length of time messages spent in the Outbreak Quarantine.

This duration is determined by the time it takes the system to compile enough data about the potential threat to make a verdict on its safety. Messages with viral threats typically spend more time in the quarantine than those with non-viral threats, because they must wait for anti-virus program updates. The maximum retention time that you specify for each mail policy is also reflected.

- The URLs most frequently rewritten to redirect message recipients to the Cisco Web Security Proxy for click-time evaluation of the site if and when the recipient clicks a potentially malicious link in a message.

This list may include URLs that are not malicious, because if any URL in a message is deemed malicious, then all URLs in the message are rewritten.



Note In order to correctly populate the tables on the Outbreak Filters reporting page, the appliance must be able to communicate with the Cisco update servers specified in Management Appliance > System Administration > Update Settings.

For more information, see the Outbreak Filters chapter.

Reporting of Graymail

Graymail statistics are reflected in the following reports:

Report	Contains the Following Graymail Data
Mail Flow Summary page > Incoming tab	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages.
Mail Flow Details page > Outgoing Senders tab	The top graymail senders.
Mail Flow Details page > Incoming Mails tab	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for all the IP addresses, domain names, or network owners.
User Mail Summary page > Top Users by Graymail	The top end users who receive graymail.
User Mail Summary page > User Mail Details	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for all the users.

Related Topics

- [Reporting of Marketing Messages after Upgrade to AsyncOS 9.5 , on page 91](#)

Reporting of Marketing Messages after Upgrade to AsyncOS 9.5

After upgrade to AsyncOS 9.5:

- The number of marketing messages is the sum of marketing messages detected before and after the upgrade.
- The total number of graymail messages does not include the number of marketing messages detected before the upgrade.
- The total number of attempted messages also includes the number of marketing messages detected before the upgrade.
- If the graymail feature is not enabled on managed Email Security appliances, marketing messages are counted as clean messages.

System Capacity Page

The **Email > Reporting > 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, on page 93](#) and [System Capacity – Outgoing Mail, on page 93](#).
- **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, on page 92](#).
- **Resource Conservation Mode:** When an 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 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. See [Resource Conservation Activity, on page 94](#).

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



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

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

Occasional spikes in the Workqueue graphs are normal and expected. If the messages in the work queue remain higher than the configured threshold for a long duration, this may indicate a capacity issue. In this scenario, consider tuning the threshold level or review the system configuration.

To change the work queue threshold level, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#).



Tip 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.

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.

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.

System Capacity – System Load

The system load report shows the following:

- [Overall CPU Usage, on page 94](#)
- [Memory Page Swapping, on page 94](#)
- [Resource Conservation Activity, on page 94](#)

Overall CPU Usage

Email Security appliances are 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.



Note This graph also indicates a threshold for CPU usage that is a visual reference only. To adjust the position of this line, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#). You can configure your Email Security appliances to send you alerts that will suggest actions that you can take to address capacity issues.

This page also shows a graph that displays the amount of CPU used by different functions, including mail processing, spam and virus engines, reporting, and quarantines. The CPU-by-function graph is a good indicator of which areas of the product use the most resources on your system. If you need to optimize your appliance, this graph can help you determine which functions may need to be tuned or disabled.

Memory Page Swapping

The memory page swapping graph shows how frequently the system must page to disk, in kilobytes per second.

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 C170 appliances). To improve performance, you may need to add Email Security appliances to your network or tune your configuration to ensure maximum throughput.



Note This graph also indicates a threshold for memory page swapping that is a visual reference only. To adjust the position of this line, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#). You can configure your Email Security appliances to send you alerts that will suggest actions that you can take to address capacity issues.

Resource Conservation Activity

The resource conservation activity graph shows the number of times the Email Security appliance entered Resource Conservation Mode (RCM). For example, if the graph shows *n* times, it means that the appliance has entered RCM *n* times and exited at least *n-1* times.

Your appliances should enter RCM infrequently and only during a very large or unusual increase in mail volume. If the Resource Conservation Activity graph shows that your appliance is entering RCS frequently, it may be an indication that the system is becoming overloaded.

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).

Threshold Indicator in System Capacity Graphs

In some graphs, a line indicates the default value that may indicate a possible problem if it is frequently or consistently crossed. To adjust this visual indicator, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#).

Reporting Data Availability Page

The **Email > Reporting > 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.

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.

Understanding the Email Reporting Pages on the New Web Interface



Note This list represents the reports available in the latest supported release of AsyncOS for Email Security appliances under the **Reports** drop-down of the web interface. For more information, see [Using the Interactive Report Pages, on page 37](#). If your Email Security appliances are running earlier releases of AsyncOS, not all of these reports are available.

Table 24: Email Reports Drop-down Options

Reports Drop-down Option	Action
Mail Flow Summary Page	The Mail Flow Summary report page provides a synopsis of the activity on your Email Security appliances. It includes graphs and summary tables for the incoming and outgoing messages. For more information, see the Mail Flow Summary Page, on page 100 .
System Capacity Page	The System Capacity report page shows detailed information about the overall workload of the reporting data, sent to the Security Management appliance. For more information, see the System Capacity Page, on page 105 .
File and Malware Reports	
Advanced Malware Protection Page (File Reputation and File Analysis)	The Advanced Malware Protection report page shows reporting views that displays details of Summary, File Reputation, File Analysis, File Retrospection and Mailbox Auto Remediation, for incoming and outgoing file-based threats. For more information, see the Advanced Malware Protection Page, on page 108 .

Reports Drop-down Option	Action
Virus Filtering Page	<p>The Virus Filtering report page provides an overview of the viruses that are sent to and from your network. This 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 Virus Filtering Page, on page 114.</p>
Macro Detection Page	<p>The Macro Detection report page shows the top incoming and outgoing macro-enabled attachments by file type detected by the content filter and message filters.</p> <p>For more information, see the Macro Detection Page, on page 116.</p>
Email Threat Reports	
DMARC Verification Page	<p>The DMARC Verification report page shows the top sender domains that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification, and a summary of the actions taken for incoming messages from each domain.</p> <p>For more information, see the DMARC Verification Page, on page 116.</p>
Outbreak Filtering Page	<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 phishing, scam, virus and malware attacks.</p> <p>For more information, see the Outbreak Filtering Page, on page 117.</p>
URL Filtering Page	<p>Use this page to view the URL categories most frequently occurring in messages, the most common URLs in spam messages, and the number of malicious and neutral URLs seen in messages.</p> <p>For more information, see the URL Filtering Page, on page 119.</p>
URL Retrospection Report Page	<p>The URL Retrospection Report page shows URLs processed by the URL Retrospective Service. This page lists the malicious URLs, date and time when verdict is received from the URL Retrospective Service, and the remediation status of impacted messages.</p> <p>For more information, see URL Retrospection Report page, on page 120.</p>
Forged Email Detection Page	<p>The Forged Email Detection report page includes the following reports:</p> <ul style="list-style-type: none"> • Top Forged Email Detection. Displays the top ten users in the content dictionary that matched the forged From: header in the incoming messages. • Forged Email Detection: Details. Displays a list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched. <p>For more information, see the Forged Email Detection Page, on page 120.</p>

Reports Drop-down Option	Action
Sender Domain Reputation Page	<p>You can use this report page to view incoming messages based on the verdict received and threat category from the SDR service</p> <p>For more information, see the Sender Domain Reputation Page, on page 121.</p>
External Threat Feeds Page	<p>The External Threat Feeds page shows the following reports:</p> <ul style="list-style-type: none"> • Top ETF sources that is used to detect threats in messages. • Top IOCs that matched threats detected in messages. • Top ETF sources that is used to filter malicious incoming mail connections <p>For more information, see the External Threat Feeds Page, on page 121.</p>
Safe Print	<p>You can use the Safe Print report page to view:</p> <ul style="list-style-type: none"> • Number of safe-printed attachments based on the file type in graphical format. • Summary of safe-printed attachments based on the file type in tabular format. <p>For more information, see the Safe Print Page , on page 80.</p>
Advanced Phishing Protection Page	<p>You can use the Advanced Phishing Protection report page to view:</p> <ul style="list-style-type: none"> • Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service. • Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service. <p>For more information, see the Advanced Phishing Protection Reports Page, on page 122.</p>
Connection and Flow Reports	
Mail Flow Details Page	<p>The Mail Flow Details report 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 Mail Flow Details Page, on page 122.</p>
Sender Groups Page	<p>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.</p> <p>For more information, see the Sender Groups Page, on page 129.</p>

Reports Drop-down Option	Action
Outgoing Destinations Page	<p>The Outgoing Destinations report 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 Outgoing Destinations Page, on page 130.</p>
TLS Encryption Page	<p>The TLS Encryption report 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 TLS Encryption Page, on page 132.</p>
Inbound SMTP Authentication Page	<p>The Inbound SMTP authentication report page shows the use of client certificates and the SMTP AUTH command to authenticate SMTP sessions between the Email Security appliance and users' mail clients.</p> <p>For more information, see the Inbound SMTP Authentication Page, on page 134.</p>
Rate Limits Page	<p>The Rate Limits report page shows the mail senders (based on MAIL-FROM address) who exceed the threshold you set for the number of message recipients per sender.</p> <p>For more information, see the Rate Limits Page, on page 136.</p>
Connections by Country Page	<p>The Connections by Country report page shows the:</p> <ul style="list-style-type: none"> • Top incoming mail connections based on country of origin in graphical format. • Total incoming mail connections and messages based on country of origin in tabular format. <p>For more information, see the Connections by Country Page, on page 137.</p>
Domain Protection Page	<p>You can use the Domain Protection report page of the new web interface of your appliance to view:</p> <ul style="list-style-type: none"> • Summary of messages that are classified as legitimate or threat, in a graphical format. • Summary of the destination domains details based on the senders, in a tabular format. <p>For more information, see the Domain Protection Page, on page 137.</p>
User Reports	

Reports Drop-down Option	Action
User Mail Summary Page	<p>The User Mail Summary report 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.</p> <p>For more information, see the User Mail Summary, on page 138.</p>
DLP Incident Summary Page	<p>The DLP Incident Summary report page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail.</p> <p>For more information, see the DLP Incident Summary Page, on page 140.</p>
Web Interaction Page	<p>The Web Interaction report page identifies the end users who clicked URLs rewritten by policy or Outbreak Filter, and the action associated with each user click.</p> <p>For more information, see the Web Interaction Page, on page 141.</p>
Remediation Reports Page	<p>You can now monitor the remediation results for Mailbox Auto Remediation and Mailbox Search and Remediate using the Remediation Report.</p> <p>This report provides a summary of:</p> <ul style="list-style-type: none"> • Total number of messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate. • Number of messages successfully remediated for a configured remedial action. • Number of messages for which the remediation failed. <p>Click the Mailbox Auto Remediation and Mailbox Search and Remediate tabs in the report to view details about the messages for which the remediation was attempted.</p> <p>For more information, see the Remediation Reports Page, on page 143</p>
Filter Reports	
Message Filters Page	<p>The Message Filters report page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages.</p> <p>For more information, see the Message Filters Page, on page 145.</p>
High Volume Mail Page	<p>The High Volume Mail report page identifies attacks involving a large number of messages from a single sender, or with identical subjects, within a moving one-hour period.</p> <p>For more information, see the High Volume Mail Page, on page 145.</p>

Reports Drop-down Option	Action
Content Filters Page	The Content Filters report 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. For more information, see the Content Filters Page, on page 146 .

Mail Flow Summary Page

The Mail Flow Summary report page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Mail Flow Summary report page includes graphs and summary tables for the incoming and outgoing messages.

The Mail Flow Summary: Incoming report page shows the incoming mail graphs for the total number of messages that are processed and blocked by the appliance, as well as the summary of the incoming mails.

You can use the mail trend graphs on this page to monitor the flow of all the incoming mails that are processed and blocked by your appliances, based on the selected time range. For more information, see [Choosing a Time Range for Reports](#), on page 26.

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#), on page 55

The following mail trend graphs provide a visual representation of the incoming mail flow:

- Threat Detection Summary
- Content Summary

You can view the mail trend of the incoming messages based on the required counters for the respective categories. For more information, see [Using Counters to Filter Data on the Trend Graphs](#), on page 41.

The Mail Flow Summary: Outgoing report page shows the outgoing mail graphs for the total number of messages that are processed and delivered by the appliance, as well as the summary of the outgoing mail.

You can use the mail trend graphs on this page to monitor the flow of all the outgoing mails that are processed and delivered by your appliances, based on the selected time range. For more information, see [Choosing a Time Range for Reports](#), on page 26.

The following mail trend graphs provide a visual representation of the mail flow of the Outgoing Mails.

You can view the mail trend of the outgoing messages based on the required counters of the processed messages. For more information, see [Using Counters to Filter Data on the Trend Graphs](#), on page 41.

The following list explains the various sections on the Mail Flow Summary report page:

Table 25: Details on the Mail Flow Summary Page

Section	Description
Mail Flow Summary: Incoming	
Number of Messages	The Number of Messages graph provides a visual representation of the total number of messages processed, including the messages that are processed as threat messages.

Section	Description
Threat Messages	The Threat Messages graph provides a visual representation of the total number of messages that are blocked by the Email Security appliance.
Threat Detection Summary	<p>The Threat Detection Summary mail trend graph provides a visual representation based on the following categories:</p> <ul style="list-style-type: none"> • Connection and Reputation Filtering: Messages that are categorized as threat by the Reputation Filtering and Invalid Recipients. • Spam Detection: Messages that are categorized as threat by the Anti-spam scanning engine. • Email Spoofing: Messages which are categorized as threat due to DMARC Verification failure. • Outbreak Threat Summary: Messages which are categorized as phishing, scam, virus or malware, by the Outbreak Filtering engine. • Attachment and Malware Detection: Messages that are categorized as threat by the Anti-virus and AMP engines. • All Categories: All the messages that are categorized as threat.
Content Summary	<p>The Content Summary mail trend graph provides a visual representation based on the following categories:</p> <ul style="list-style-type: none"> • Graymail: Messages that are categorized as marketing, bulk or social networking. • Content Filters: Messages that are categorized by the content filters. • All Categories: All the messages that are categorized by graymail engines and content filters.
Mail Flow Summary: Outgoing	
Number of Messages	The Number of Messages graph provides a visual representation of the total number of messages processed, including the messages that are processed as clean.
Message Delivery	The Message Delivery graph provides a visual representation of the total number of messages that are delivered, including hard bounces.

Section	Description
Outgoing Mails	<p>The Outgoing Mails trend graph provides a visual representation based on the following categories:</p> <ul style="list-style-type: none"> • Spam Detected • Virus Detected • Detected by AMP • Stopped by Content Filters • Stopped by DLP

Related Topics

- [How Email Messages Are Categorized by the Appliances, on page 63](#)
- [How Incoming Mail Messages are Counted, on page 63](#)
- [Categorizing Email Messages on the Mail Flow Summary Page, on page 103](#)

How Incoming Mail Messages are Counted

Counts of incoming messages are 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 sender 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 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 precedence of the various filters and scanning activities greatly impacts the results of message processing.

In the example above, the various verdicts follow these rules of precedence:

- 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.

Alternately, if the message were quarantined by Outbreak Filters, it would not be counted until it was released from the quarantine and again processed through the work queue.

For complete information about message processing precedence, see chapter about the email pipeline in the online help or user guide for your Email Security appliance.

Categorizing Email Messages on the Mail Flow Summary Page

Incoming messages that are considered as threat, and outgoing messages that are delivered in the Mail Flow Summary report page are categorized as follows:

Table 26: Email Categories on Mail Flow Summary Page

Category	Description
Mail Flow Summary: Incoming	
Reputation Filtering	<p>All connections blocked by HAT policies, multiplied by a fixed multiplier, (see the How Incoming Mail Messages are Counted, on page 63) and added with all recipients blocked by recipient throttling.</p> <p>The value for Stopped by IP Reputation Filtering is calculated based on the following factors:</p> <ul style="list-style-type: none"> • Number of “throttled” messages from this sender. • Number of rejected or TCP refused connections (may be a partial count). • A conservative multiplier for the number of messages per connection. <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 an indicative value of the least number of messages are stopped.</p> <p>The Reputation Filtering total count and percentage on the Mail Flow Summary report page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.</p>
Invalid Recipients	The total count and percentage of all mail recipients rejected by conversational LDAP rejection in addition to all RAT rejections.
Anti-Spam	The total count and percentage of incoming messages detected by the anti-spam scanning engine as positive or suspect. Additionally, messages that are both spam and virus positive.

Category	Description
Anti-Virus	<p>The total count and percentage of incoming messages detected as virus positive and not also spam.</p> <p>The following messages are counted in the “Virus Detected” category:</p> <ul style="list-style-type: none"> • Messages with a virus scan result of “Repaired” or “Infectious” • Messages with a virus scan result of “Encrypted” when the option to count encrypted messages as containing viruses is selected • Messages with a virus scan result of “Unscannable” when the action for unscannable messages is NOT “Deliver” • Messages with a virus scan result of “Unscannable” or “Encrypted” when the option to deliver to an alternate mail host or an alternate recipient is selected • Messages that are deleted from the Outbreak quarantine, either manually or by timing out.
Advanced Malware Protection	<p>The total count and percentage of incoming messages blocked by the file analysis service.</p> <p>A message attachment was found to be malicious by file reputation filtering. This value does not include verdict updates or files found to be malicious by file analysis.</p>
Content Filter	The total count and percentage of incoming messages that are stopped by message and content filters.
DMARC Policy	The total count and percentage of incoming messages that failed DMARC verification policy.
S/MIME Verification/Decryption Failed	The total count and percentage of incoming messages that failed S/MIME verification, decryption, or both.
Mail Flow Summary: Outgoing	
Hard Bounces	The total count and percentage of outgoing messages that are permanently undeliverable.
Delivered	The total count and percentage of outgoing messages that are delivered.



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.

Related Topics

[Mail Flow Details Page, on page 122](#)

System Capacity Page

The System Capacity report 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 report 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.

To view the System Capacity report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > System Capacity** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

You can 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, on page 93](#) and [System Capacity – Outgoing Mail, on page 93](#).
- **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, on page 92](#).
- **Resource Conservation Mode:** When an 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 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. See [Resource Conservation Activity, on page 94](#).

Related Topics

- [How to Interpret the Data You See on System Capacity Page, on page 92](#)
- [System Capacity – Workqueue, on page 92](#)
- [System Capacity – Incoming Mail, on page 93](#)
- [System Capacity – Outgoing Mail, on page 93](#)
- [System Capacity – All, on page 94](#)
- [Threshold Indicator in System Capacity Graphs, on page 95](#)

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



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

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

Occasional spikes in the Workqueue graphs are normal and expected. If the messages in the work queue remain higher than the configured threshold for a long duration, this may indicate a capacity issue. In this scenario, consider tuning the threshold level or review the system configuration.

To change the work queue threshold level, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#).



Tip 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.

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.

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.

System Capacity – System Load

The system load report shows the following:

- [Overall CPU Usage, on page 94](#)
- [Memory Page Swapping, on page 94](#)
- [Resource Conservation Activity, on page 94](#)

Overall CPU Usage

Email Security appliances are 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.



Note This graph also indicates a threshold for CPU usage that is a visual reference only. To adjust the position of this line, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#). You can configure your Email Security appliances to send you alerts that will suggest actions that you can take to address capacity issues.

This page also shows a graph that displays the amount of CPU used by different functions, including mail processing, spam and virus engines, reporting, and quarantines. The CPU-by-function graph is a good indicator of which areas of the product use the most resources on your system. If you need to optimize your appliance, this graph can help you determine which functions may need to be tuned or disabled.

Memory Page Swapping

The memory page swapping graph shows how frequently the system must page to disk, in kilobytes per second.

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 C170 appliances). To improve performance, you may need to add Email Security appliances to your network or tune your configuration to ensure maximum throughput.



Note This graph also indicates a threshold for memory page swapping that is a visual reference only. To adjust the position of this line, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#). You can configure your Email Security appliances to send you alerts that will suggest actions that you can take to address capacity issues.

Resource Conservation Activity

The resource conservation activity graph shows the number of times the Email Security appliance entered Resource Conservation Mode (RCM). For example, if the graph shows *n* times, it means that the appliance has entered RCM *n* times and exited at least *n*-1 times.

Your appliances should enter RCM infrequently and only during a very large or unusual increase in mail volume. If the Resource Conservation Activity graph shows that your appliance is entering RCS frequently, it may be an indication that the system is becoming overloaded.

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).

Threshold Indicator in System Capacity Graphs

In some graphs, a line indicates the default value that may indicate a possible problem if it is frequently or consistently crossed. To adjust this visual indicator, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances, on page 525](#).

Advanced Malware Protection Page

Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.
- Evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

This feature is available for incoming and outgoing messages.

For more information on the file reputation filtering and file analysis, see the *User Guide or Online Help for AsyncOS for Email Security Appliances*.

To view the report page, select **Advanced Malware Protection** from the Filter and Malware Reports section of the Reports drop-down.

The Advanced Malware Protection report page shows the following reporting views:

- [Advanced Malware Protection – Summary, on page 109](#)

- [Advanced Malware Protection – AMP Reputation, on page 109](#)
- [Advanced Malware Protection – File Analysis, on page 110](#)
- [Advanced Malware Protection – File Retrospection, on page 111](#)
- [Advanced Malware Protection – Mailbox Auto Remediation, on page 111](#)

To view the Advanced Malware Protection report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Advanced Malware Protection** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The Advanced Malware Protection report page displays a metrics bar that provides real time data of all the managed appliances connected to the Cisco Threat Grid appliance.

**Note**

- You must use the `trailblazerconfig > enable` command on the CLI to populate data on the metrics bar. For more information, see [The trailblazerconfig Command, on page 518](#).
- You can only view the data from the Cisco Threat Grid appliance for the day, week and month.

Related Topics

- [Identifying Files by SHA-256 Hash , on page 84](#)
- [Requirements for File Analysis Report Details , on page 82](#)
- [Viewing File Reputation Filtering Data in Other Reports , on page 86](#)

Advanced Malware Protection – Summary

The Advanced Malware Protection - Summary page shows the complete summary of the incoming and outgoing file-based threats that are identified by the file reputation and file analysis service.

For more information, see [Advanced Malware Protection – AMP Reputation, on page 109](#) and [Advanced Malware Protection – File Analysis, on page 110](#).

Advanced Malware Protection – AMP Reputation

The Advanced Malware Protection - AMP Reputation page shows incoming and outgoing file-based threats that were identified by the file reputation service.

For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.

If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.

The **Incoming files handled by AMP** section shows the incoming malware files by different categories such as malicious, clean, unknown, unscannable, and low risk.

Incoming malicious files are categorized as the following:

- The percentage of blocked listed file SHAs received from the AMP reputation server that are categorized as **Malware**.

- The percentage of blocked listed file SHAs received from the AMP for Endpoints console that are categorised as **Custom Detection**. The threat name of a blocked listed file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report.
- The percentage of blocked listed file SHAs based on the threshold settings that are categorised as **Custom Threshold**.

You can click on the link in the More Details section of the report to view the file trajectory details of a blocked listed file SHA in the AMP for Endpoints console.

You can view the **Low Risk** verdict details in the Incoming Files Handed by AMP section of the report.

You can use the AMP Reputation view of the Advanced Malware Protection: Incoming report page to view:

- The summary of incoming files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- A trend graph for all the incoming malware threat files based on the selected time range.
- The top incoming malware threat files.
- The top incoming threat files based on the file types.
- The Incoming Malware Threat Files interactive table that lists the top incoming malware threat files.

Drill down to view detailed analysis results, including the threat characteristics for each file.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

You can use the AMP Reputation view of the Advanced Malware Protection: Outgoing report page to view:

- The summary of outgoing files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- A trend graph for all the outgoing malware threat files based on the selected time range.
- The top outgoing malware threat files.
- The top outgoing threat files based on the file types.
- The Outgoing Malware Threat Files interactive table that lists the top outgoing malware threat files that are identified by the file reputation service.

Drill down to view detailed analysis results, including the threat characteristics for each file.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

Advanced Malware Protection – File Analysis

The Advanced Malware Protection - File Analysis page shows the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.

To view more than 1000 File Analysis results, export the data as a .csv file.

For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are included in the allowed list on the AMP Threat Grid appliance show as "clean". For information about allowed list, see the AMP Threat Grid documentation or online help.

Drill down to view detailed analysis results, including the threat characteristics for each file.

You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file. For more information, see [Identifying Files by SHA-256 Hash](#), on page 84.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click the **Details** link in the table.

To view details on the server that analyzed a file, see [Requirements for File Analysis Report Details](#), on page 82.

If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.

You can use the File Analysis view of the Advanced Malware Protection report page to view:

- The number of incoming and outgoing files that are uploaded for file analysis by file analysis service of the Advanced Malware Protection engine.
- A list of incoming and outgoing files that have completed file analysis requests.
- A list of incoming and outgoing files that have pending file analysis requests.

Advanced Malware Protection – File Retrospection

The Advanced Malware Protection - File Retrospection page lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about on this scenario, see the documentation for your Email Security appliance.

As Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data might unviel more information.

To view more than 1000 verdict updates, export the data as a .csv file.

In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.

To view all affected messages for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click a SHA-256 link.

You can use the File Retrospection view of the Advanced Malware Protection report page to view:

- A list of incoming and outgoing files with retrospective verdict changes.

Advanced Malware Protection – Mailbox Auto Remediation

The Advanced Malware Protection - Mailbox Auto Remediation report page shows the details of the mailbox remediation results for the incoming files.

You can use the Advanced Malware Protection - Mailbox Auto Remediation page to view retrospective security details such as:

- The filenames associated with a SHA-256 hash.

- Remedial actions taken on messages.
- A list of recipients for whom the mailbox remediation was successful or unsuccessful.

The Recipients for whom remediation was unsuccessful field is updated in the following scenario:

- There was a connectivity issue between your appliance and Office 365 services when the appliance was trying to perform the configured remedial action.

Click on a SHA-256 hash to view the related messages in Message Tracking.

Requirements for File Analysis Report Details

- [\(Cloud File Analysis\) Ensure That the Management Appliance Can Reach the File Analysis Server](#), on page 82
- [\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#), on page 82
- [\(On-Premises File Analysis\) Activate the File Analysis Account](#), on page 83
- [Additional Requirements](#), on page 83

(Cloud File Analysis) Ensure That the Management Appliance Can Reach the File Analysis Server

In order to obtain File Analysis report details, the appliance must be able to connect to the File Analysis server over port 443. See details in [Firewall Information, on page 621](#)

(Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results

In order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization, you need to join all appliances to the same appliance group.



Note If you load a license keys file that does not contain the 'cloud admin feature' key in the on-premises virtual email gateway, you can still perform auto-registration of Threat Group File Analysis using the Smart License Account ID.

-
- Step 1** In the Legacy Web Interface, click **Management Appliance > Centralized Services > Security Appliances** and scroll down to the File Analysis section.
- Step 2** If your managed appliances are pointed at different File Analysis cloud servers, select the File Analysis server from which to display result details.
- Result details will not be available for files processed by any other cloud server.
- Step 3** [Applicable if Smart Licensing is disabled on Cisco Secure Email and Web Manager] Enter the group name for file analysis reporting in the **Group Name** field and click **Group Now**.
- Or
- [Applicable if Smart Licensing is enabled on Cisco Secure Email and Web Manager] The system automatically registers the Smart Account ID as the group ID and displays it in the **Group Name** field.
- Step 4** Configure the same group ID on each managed appliance that will share data with this appliance.

Notes:

- You can modify the group name at any time. Edit the name and click **Group Now**. This change takes effect immediately; it does not require a Commit.
- This group name is case-sensitive. This value must be identical on all appliances that will share data about files that are uploaded for analysis.
- It is suggested to use your CCOID for this value.
- An appliance can belong to only one group.
- You can add a machine to a group at any time, but you can add it only once.
- If Smart Licensing is enabled, the appliances are grouped using the Smart Account ID.

What to do next**Related Topics**

[For Which Files Are Detailed File Analysis Results Visible in the Cloud? , on page 86](#)

(On-Premises File Analysis) Activate the File Analysis Account

If you have deployed an on-premises (private cloud) Cisco AMP Threat Grid Appliance, you must activate the File Analysis account for your Cisco Content Security Management appliance in order to view report details available on the Threat Grid appliance. You generally only need to do this once.

Before you begin

Ensure that you are receiving System alerts at Critical level.

Step 1 The first time you attempt to access File Analysis report details from the Threat Grid appliance, wait a few minutes and you will receive an alert that includes a link.

If you do not receive this alert, go to **Management Appliance > System Administration > Alerts** and click **View Top Alerts**.

Step 2 Click the link in the alert message.

Step 3 Activate your management appliance account.

Additional Requirements

For any additional requirements, see the Release Notes for your Security Management appliance release, available from <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are

recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format).

Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A Detected by Advanced Malware Protection column may be hidden by default in applicable reports. To display additional columns, click the Columns link at the bottom of the table.

For Which Files Are Detailed File Analysis Results Visible in the Cloud?

If you have deployed public-cloud File Analysis, you can view detailed results for all files uploaded from any managed appliance that has been added to the appliance group for File Analysis.

If you have added your management appliances to the group, you can view the list of managed appliances in the group by clicking the **View Appliances in Group** button on the **Management Appliance > Centralized Services > Security Appliances > File Analysis** page.

Appliances in the analysis group are identified by the File Analysis Client ID. To determine this identifier for a particular appliance, look in the following location:

Appliance	Location of File Analysis Client ID
Email Security appliance	Advanced Settings for File Analysis section on the Security Services > File Reputation and Analysis page.
Web Security appliance	Advanced Settings for File Analysis section on the Security Services > Anti-Malware and Reputation page.
Cisco Content Security Management appliance	At the bottom of the Management Appliance > Centralized Services > Security Appliances page.

Related Topics

- [\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#), on page 82

Virus Filtering Page

The Virus Filtering report 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.

To view the Virus Filtering report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Virus Filtering** from the Reports drop-down. For more information, see [Using the Interactive Report Pages](#), on page 37.

If you run multiple virus scanning engines, the Virus Filtering report 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 Filtering report page:

Table 27: Details on the Virus Filtering Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports , on page 26.
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group , on page 25.
Top Incoming Virus Types Detected	This section displays a chart view of the detected viruses in messages sent to your network.
Top Outgoing Virus Types Detected	This section displays a chart view of the detected viruses in messages sent from your network.
Virus Types Detail	An interactive table that shows the details of each virus type. For more information, see Virus Types Detail Table , on page 115



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 messages. Similarly, to see which IP addresses have sent virus positive emails within your network, go to the Outgoing Senders page and sort by virus positive messages.

From the Virus Filtering report page, you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data](#) , on page 31.

You can generate a scheduled report for the Virus Filtering report page. See the [Scheduling Email Reports](#), on page 152.

Virus Types Detail Table

The Virus Types Detail table is an interactive table that shows the total number of virus-infected messages, with a breakdown by incoming and outgoing messages. Click the column headings to sort the data.

The following table shows the table column descriptions for the Virus Types Detail table:

Table 28: Table Column Descriptions for Virus Types Detail Table

Column Name	Description
Virus Type	The name of the virus type.
Incoming Messages	Number of incoming messages detected as virus.
Outgoing Messages	Number of outgoing messages detected as virus.

Column Name	Description
Total Infected Messages	Total number of infected messages (incoming and outgoing).

Macro Detection Page

You can use the Macro Detection report page to view:

- Top Incoming Macro-Enabled Attachments by File Type in graphical and tabular format.
- Total Incoming Macro-Enabled Attachments by File Type in tabular format.
- Top Outgoing Macro-Enabled Attachments by File Type in graphical and tabular format.
- Total Outgoing Macro-Enabled Attachments by File Type in tabular format.

To view the Macro Detection report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Macro Detection** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the Macro Detection report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

You can click on the number of macro-enabled attachments to view the related messages in Message Tracking.



Note During report generation:

- If one or more macros are detected within an archive file, the Archive Files file type is incremented by one. The number of macro-enabled attachments within an archive file are not counted.
 - If one or more macros are detected within an embedded file, the parent file type is incremented by one. The number of macro-enabled attachments within an embedded file are not counted.
-

DMARC Verification Page

The DMARC Verification report page shows the top sender domains that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification, and a summary of the actions taken for incoming messages from each domain. You can use this report to fine-tune your DMARC settings and answer these kinds of questions:

- Which domains sent the most messages that failed DMARC verification?
- For each domain, what actions are taken on messages that failed DMARC verification?

You can use the DMARC Verification report page to view:

- Top Domains by DMARC verification failures in graphical format.
- Total domains by DMARC verification details in tabular format. For more information, see [Domains by DMARC Verification Details Table, on page 117](#).

To view the DMARC Verification report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > DMARC Verification** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

From the DMARC Verification report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

For more information about DMARC verification, see the Email Authentication chapter in the online help or user guide for your Email Security appliance.

Domains by DMARC Verification Details Table

The Domains by DMARC Verification Details table is an interactive table that shows the details of the sender domains that have failed (by either being rejected, quarantined, or no action), attempted, and passed the Domain-based Message Authentication, Reporting and Conformance (DMARC) verification.

To customize and sort information on the table, see [Customizing Tables on Report Pages , on page 40](#).

To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

Outbreak Filtering Page

The Outbreak Filtering report 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 Filtering report page to answer the following types of questions:

- How many messages are quarantined and by which Outbreak Filters rule?
- How long do messages stay in the Outbreak Quarantine?
- Which potentially malicious URLs are most frequently seen?

To view the Outbreak Filtering report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Outbreak Filtering** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The following table explains the various sections on the Outbreak Filtering report page:

Table 29: Details on the Outbreak Filtering Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports , on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .

Section	Description
Threats By Type	The Threats by Type section shows the different types of threat messages received by the appliance.
Threat Summary	<p>The Threat Summary section shows a breakdown of the messages by Malware, Phish, Scam and Virus.</p> <p>To view Message Tracking details for the messages that populate this report, click a blue number link in the table.</p>
Threat Details	<p>The Threat Details interactive table shows details about specific outbreaks, including the threat category (virus, scam, or phishing), threat name, a description of the threat, and the number of messages identified.</p> <p>To view Message Tracking details for the messages that populate this report, click a blue number link in the table.</p>
Hit Messages from Incoming Messages	<p>The Hit Messages from Incoming Messages section shows the chart and summary of the number of incoming messages processed by Outbreak Filters in the selected time period.</p> <p>Non-viral threats include phishing emails, scams, and malware distribution using links to an external website.</p>
Hit Messages by Threat Level	<p>The Hit Messages by Threat Level section shows the chart and summary of the severity of threats caught by Outbreak Filters.</p> <p>Level 5 threats are severe in scope or impact, while Level 1 represents low threat risk. For descriptions of threat levels, see the online help or user guide for your Email Security appliance.</p>
Messages resided in Outbreak Quarantine	<p>The Messages resided in Outbreak Quarantine shows the length of time messages spent in the Outbreak Quarantine.</p> <p>This duration is determined by the time it takes the system to compile enough data about the potential threat to make a verdict on its safety. Messages with viral threats typically spend more time in the quarantine than those with non-viral threats, because they must wait for anti-virus program updates. The maximum retention time that you specify for each mail policy is also reflected.</p>
Top URL's Rewritten	<p>The Top URL's Rewritten section shows the URLs that are most frequently rewritten to redirect message recipients to the Cisco Web Security Proxy for click-time evaluation of the site if and when the recipient clicks a potentially malicious link in a message.</p> <p>This list may include URLs that are not malicious, because if any URL in a message is deemed malicious, then all URLs in the message are rewritten.</p> <p>To view Message Tracking details for the messages that populate this report, click a blue number link in the table.</p>



Note In order to correctly populate the tables on the Outbreak Filtering report page, the appliance must be able to communicate with the Cisco update servers.

For more information, see the Outbreak Filters chapter in the online help or user guide for your Email Security appliance.

URL Filtering Page

URL Filtering reports are available for incoming and outgoing messages.

Only messages that are scanned by the URL filtering engine (either as part of anti-spam/outbreak filter scanning or through message/content filters) are included in these modules. However, not all of the results are necessarily specifically attributable to the URL Filtering feature.



Note URL Filtering report modules are populated only if URL filtering is enabled.

From the URL Filtering report page, you can view:

- The Top URL Categories module includes all categories found in messages that have been scanned, whether or not they match a content or message filter.

Each message can be associated with only one reputation level. For messages with multiple URLs, the statistics reflect the lowest reputation of any URL in the message.

- The Top URL spam messages

URLs in the global allowed list configured at **Security Services > URL Filtering** page of the email security appliance, are not included in reports.

URLs in allowed lists used in individual filters are included in reports.

- Malicious URLs are URLs that Outbreak Filters have determined to have poor reputation. Neutral URLs are those that Outbreak Filters have determined to require click-time protection. Neutral URLs have therefore been rewritten to redirect them to the Cisco Web Security proxy.

Results of URL category-based filters are reflected in content and message filter reports.

Results of click-time URL evaluations by the Cisco Web Security proxy are not reflected in reports.

To view the URL Filtering report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > URL Filtering** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The following table explains the various sections on the URL Filtering report page:

Table 30: Details on the URL Filtering Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports , on page 26.

Section	Description
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .
Top URL Categories	This section displays the graphical view and summary of the top URL categories of the incoming and outgoing messages. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.
Top URL Spam Messages	This section displays the graphical view and summary of the top incoming and outgoing URL spam messages.
Malicious and Neutral URLs	This section displays the chart view and the summary of malicious and neutral URLs of the incoming and outgoing messages. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

From the URL Filtering report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

URL Retrospection Report page

The URL Retrospection Report page shows URLs processed by the URL Retrospective Service. It displays the following details:

- **URL** - The URLs sent to the URL Retrospective Service analysis by Cisco Secure Email Cloud Gateway.
- **Verdict Received** - Date and time when Cisco Secure Email Cloud Gateway receives a verdict from the URL Retrospective Service.
- **Remediation Status of Impacted Messages** - Action taken for the malicious URLs and the number of messages against each remediation status. The possible remediation statuses are: In- Progress, Success, Failed, and Skipped.

Forged Email Detection Page

The Forged Email Detection page includes the following reports:

- **Top Forged Email Detection.** Displays the top ten users in the content dictionary that matched the forged From: header in the incoming messages.
- **Forged Email Detection: Details.** Displays a list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched.

To view the Forged Email Detection report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Forged Email Detection** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The Forged Email Detection reports are populated only if you are using the Forged Email Detection content filter or the `forged-email-detection` message filter.

From the Forged Email Detection report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data](#), on page 31.

Sender Domain Reputation Page

You can use the Sender Domain Reputation report page to view:

- Incoming messages based on the verdict received from the SDR service in graphical format.
- Summary of incoming messages based on the threat category and verdict received from the SDR service in tabular format.
- Incoming messages based on the threat category received from the SDR service in graphical format.



Note Only the messages whose SDR verdict is 'untrusted' or 'questionable' are classified under the SDR threat category, such as, 'spam,' 'malicious,' etc.

- Summary of incoming messages based on the threat category received from the SDR service in tabular format.

To view the Sender Domain Reputation report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Sender Domain Reputation** from the Reports drop-down. For more information, see [Using the Interactive Report Pages](#), on page 37.

External Threat Feeds Page

You can use the External Threat Feeds report page to view:

- Top ETF sources used to detect threats in messages in graphical format
- Summary of ETF sources used to detect threats in messages in tabular format.
- Top IOCs that matched threats detected in messages in graphical format.
- Top ETF sources used to filter malicious incoming mail connections in graphical format.
- Summary of ETF sources used to filter malicious incoming mail connections in tabular format.

In the 'Summary of External Threat Feed Sources' section:

- You can click on the number of messages for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular threat feed source to view the distribution of the ETF source based on the IOCs.

In the 'Summary of Indicator of Compromise (IOC) Matches' section:

- You can click on the number of IOCs for a particular ETF source to view the related messages in Message Tracking.

- You can click on a particular IOC to view the distribution of the IOC based on the ETF sources.

To view the External Threat Feeds report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > External Threat Feeds** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

Safe Print Page

You can use the Safe Print Action report page to view:

- Number of safe-printed attachments based on the file type in graphical format.
- Summary of safe-printed attachments based on the file type in tabular format.

In the 'Summary of Safe Print File Types' section, click the total number of safe-printed attachments to view the message details in Message Tracking.

Advanced Phishing Protection Reports Page

You can view the following on the Advanced Phishing Protection report page:

- Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service.
- Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service.



Note If the forwarding of message metadata has failed, you must validate the configurations of the Advanced Phishing Protection feature. For more information, see the "Integrating Cisco Email Security Gateway with the Cisco Advanced Phishing Protection" chapter of the *User Guide for AsyncOS for Cisco Email Security Appliances*.

To view the Advanced Phishing Protection report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Advanced Phishing Protection** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

You can use the Advanced Phishing Protection report page to view:

- Total number of messages attempted to be forwarded to the Cisco Advanced Phishing Protection cloud service.
- Summary of messages forwarded to the Cisco Advanced Phishing Protection cloud service in a graphical format.

Mail Flow Details Page

The Mail Flow Details report 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 gather information about the IP addresses and domains of the outgoing senders.

To view the Mail Flow Details report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Mail Flow Details** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The Mail Flow Details report page has the following tabs:

- Incoming Mails
- Outgoing Senders

To search for specific information within your data, see [Searching and the Interactive Email Report Pages, on page 55](#).

From the Incoming Mails tab, you can:

- View the top senders by total threat messages in graphical format.
- View the top senders by clean messages in graphical format.
- View the top senders by graymail messages in graphical format.
- See the IP addresses, domains, or network owners (organizations) that have sent mail to your Security Management appliances.
- See detailed statistics on senders that have sent mail to your appliances. The statistics include the number of connections (accepted or rejected), attempted messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth), total threat messages, total graymails and clean messages.
- See the Incoming Mails interactive table for the detailed information about the particular IP address, domain, or network owner (organization). For more information, see [Incoming Mails Table, on page 125](#).

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a number hyperlink in the table.

From the Outgoing Senders tab, you can:

- View the top senders by total threat messages in graphical format.
- View the top senders by clean messages in graphical format.
- View the top senders (by IP address or domain) of outgoing threat messages (spam, antivirus, etc.) in your organization.
- See detailed statistics on senders that have sent mail from your appliances. The statistics include the total threat messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth) and clean messages.
- See the Sender Details interactive table for detailed information about the particular IP address or domain. For more information, see [Sender Details Table, on page 128](#).

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a number hyperlink in the table.

Related Topics

- [“No Domain Information” Link, on page 67](#)
- [Time Ranges in the Mail Trend Graphs, on page 68](#)
- [Views Within the Mail Flow Details Page, on page 124](#)
- [Incoming Mails Table, on page 125](#)
- [Sender Details Table, on page 128](#)

Views Within the Mail Flow Details Page

The Mail Flow Details: Incoming report 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 table of the Mail Flow Details page, you can click on a Sender’s 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, on page 68](#).



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 Mail Flow Details page that is specific to a particular IP address, domain, or network owner.

See the [Incoming Mails Table, on page 125](#) for an explanation of the data included in the Incoming Mails interactive table.

From the Mail Flow Details page you can export raw data to a CSV file.

The Mail Flow Details: Outgoing report page has two different views:

- IP Addresses
- Domains

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

Depending on the view you select, the Sender Details interactive table displays the top IP addresses or domains of the senders that have sent mail from the public listeners configured from the Email Security appliances. You can monitor the flow of all mail from your appliances.

See the [Sender Details Table, on page 128](#) for an explanation of the data included in the Sender Details interactive table.

"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 documentation or online help for your Email Security appliance.

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 Reports](#) , on page 26.

Incoming Mails Table

The interactive Incoming Mails table at the bottom of the Mail Flow Details: Incoming Mails 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.

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 user guide or online help for AsyncOS Email Security appliance.

For senders, that is Network Owner, IP Address or Domain, listed in the first column of the Incoming Mails 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 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, on page 68](#).

You can also view the Sender Groups report, by clicking Sender Groups report at the bottom of the Mail Flow Details page. For more information about the Sender Groups report page, see the [Sender Groups Page, on page 129](#).

To view Message Tracking details for the messages that populate this report, click a number hyperlink in the table.

The following table shows the table column descriptions for the Incoming Mails table:

Table 31: Table Column Descriptions for Incoming Mail Table

Column Name	Description
Sender Domain (Domains)	The domain name of the sender.
Sender IP Address (IP Addresses)	The IP address of the sender.
Hostname (IP Addresses)	The hostname of the sender.

Column Name	Description
DNS Verified (IP Addresses)	The IP addresses that are verified by the DNS.
SBRS (IP Addresses)	The SenderBase Reputation Score of the sender.
Last Sender Group (IP Addresses)	The details of the last sender group.
Last Sender Group (IP Addresses)	The details of the last sender group.
Network Owner (Network Owners)	The network owner of the sender.
Connections Rejected (Domains and Network Owners)	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 (Domains and Network Owners)	All connections accepted,
Total Attempted	All accepted and blocked connections attempted.
Stopped by Recipient Throttling (Domains and Network Owners)	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.
Stopped by IP Reputation Filtering	<p>The value for Stopped by IP Reputation Filtering is calculated based on several factors:</p> <ul style="list-style-type: none"> • Number of “throttled” messages from this sender • Number of rejected or TCP refused connections (may be a partial count) • A conservative multiplier for the number of messages per connection. <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 are stopped.</p> <p>Note The Reputation Filtering total on the Mail Flow Summary page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.</p>
Stopped by Domain Reputation Filtering	The total count of messages blocked based on the reputation verdict of the sender domain.

Column Name	Description
Stopped as Invalid Recipients	All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.
Spam Detected	Any spam that has been detected.
Virus Detected	Any viruses that have been detected
Detected by Advanced Malware Protection	The total count of messages detected by Advanced Malware Protection engines.
Stopped by Content Filter	The total count of messages that are stopped by a content filter.
Stopped by DMARC	The total count of messages that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification.
Total Threat	Total number of threat messages (stopped by reputation, stopped as invalid recipient, spam, plus virus)
Marketing	Number of messages detected as unwanted marketing messages.
Social	Number of messages detected as social messages.
Bulk	Number of messages detected as bulk.
Total Graymails	Number of messages detected as graymails.
Clean	All clean messages. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.

Sender Profile Pages

When you click a sender in the Incoming Mail interactive table, on the **Mail Flow Details** [New Web Interface] or **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 Mail Flow Details 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.

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.

Sender Details Table

The interactive Sender Details table at the bottom of the Mail Flow Details: Outgoing page lists the top senders that have connected to public listeners on the Email Security appliances. The table shows domains or IP addresses, based on the view selected.

To view Message Tracking details for the messages that populate this report, click a number hyperlink in the table.

The following table shows the table column descriptions for the Sender Details table:

Table 32: Table Column Descriptions for Sender Details Table

Column Name	Description
Sender Domain (Domains)	The domain name of the sender.
Sender IP Address (IP Addresses)	The IP address of the sender.
Hostname (IP Addresses)	The hostname of the sender.
Spam Detected	Any spam that has been detected.
Virus Detected	Any viruses that have been detected.
Detected by Advanced Malware Protection	The total count of messages detected by Advanced Malware Protection engines.
Stopped by Content Filter	The total count of messages that are stopped by a content filter.
Stopped by DLP	The total count of messages that are stopped by DLP engine.
Total Threat	Total number of threat messages (spam, virus)
Clean	All clean messages. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.
Total Messages	The total count of all the messages.

Sender Groups 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 documentation or online help for your Email Security appliance.

To view the Sender Groups report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Sender Groups** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the Sender Group report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).



Note You can generate a scheduled report for the Sender Group report page. See the [Scheduling Email Reports, on page 152](#).

Outgoing Destinations Page

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

You can use the Outgoing Destinations page to view:

- Which domains are the Email Security appliances sending messages to?
- How much message is sent to each domain?
- How much of that message is clean, spam-positive, virus-positive, malware 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 report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Outgoing Destinations** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

To search for specific information within your data, see [Searching and the Interactive Email Report Pages, on page 55](#).

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

Table 33: Details on the Outgoing Destinations Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports, on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .
Top Destinations by Total Threat Messages	The top destination domains of outgoing threat messages (spam, antivirus, etc.) sent by your organization. Total threat messages include spam or virus positive, or the messages that are triggered by a content filter.
Top Destinations by Clean Messages	The top destination domains of clean outgoing messages sent by your organization.
Outgoing Destinations Details	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. For more information, see Outgoing Destinations Detail Table, on page 131 . To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

From the Outgoing Destinations report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data, on page 31](#).

You can generate a scheduled report for the Outgoing Destinations page. See the [Scheduling Email Reports, on page 152](#).

Related Topics

[Outgoing Destinations Detail Table, on page 131](#)

Outgoing Destinations Detail Table

The Outgoing Destinations Detail table is an interactive table that shows the total number of messages that are processed and delivered, with a breakdown of the messages that are processed as threat (Spam, Virus, etc.) or clean, and the messages that are either hard bounced or delivered. Click the column headings to sort the data.

To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

The following table shows the table column descriptions for the Outgoing Destination Detail table:

Table 34: Table Column Descriptions for Outgoing Destination Detail Table

Column Name	Description
Destination Domain	The name of the destination domain.
Spam Detected	Number of messages detected as spam.
Virus Detected	Number of messages detected as spam.
Stopped by Content Filter	Number of messages stopped by content filters.
Total Threat	Total number of messages detected as threat (Spam, Virus, etc.)
Clean	Number of messages detected as clean,
Total Processed	Total number of messages processed as threat or clean.
Hard Bounces	<p>Number of messages that are marked as permanently undeliverable.</p> <p>Note Only the following bounce types are included while counting the hard-bounced messages:</p> <ul style="list-style-type: none"> • FiveXX hard bounce • Filter hard bounce • Other hard bounce • DNS hard bounce • Expired hard bounce
Delivered	Number of messages that are delivered.
Total Messages Delivered	Total number of messages that are delivered (including Hard Bounces).

TLS Encryption Page

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

To view the TLS Encryption report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > TLS Encryption** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The TLS Encryption report page has the following tabs:

- Incoming
- Outgoing

To search for specific information within your data, see [Searching and the Interactive Email Report Pages, on page 55](#).

The following list explains the various sections on the TLS Encryption report page:

Table 35: Details on the TLS Encryption Page

Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports, on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .

TLS Connections Graph	<p>The TLS Encryption: Incoming page displays a graph view of incoming encrypted and unencrypted TLS connections over the last hour, day, week, month or year depending on the time frame that you have selected.</p> <p>The TLS Encryption: Outgoing page displays a graph view of outgoing encrypted and unencrypted TLS connections over the last hour, day, week, month, or year, depending on the time frame that you have selected.</p>
TLS Connections Summary	<p>The TLS Encryption: Incoming page displays a table view of the total volume of incoming messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed incoming TLS encrypted messages.</p> <p>The TLS Encryption: Outgoing page displays a table view of the total volume of outgoing messages, the volume of encrypted and unencrypted messages, the volume of successful and failed outgoing TLS encrypted messages, and the volume of successful and failed outgoing TLS connection with DANE support.</p>
TLS Messages	<p>The TLS Encryption: Incoming page displays a chart view of the total count and percentage of incoming TLS encrypted and unencrypted messages.</p> <p>The TLS Encryption: Outgoing page displays a chart view of the total count and percentage of outgoing TLS encrypted and unencrypted messages.</p>
TLS Messages Summary	<p>This table displays a summary of the total count and percentage of incoming and outgoing TLS encrypted and unencrypted messages.</p>
TLS Connections Details	<p>This 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 are successful or failed. You can also view the percentage of successful and failed connections for each domain.</p> <p>For more information, see TLS Connections Details Table, on page 134.</p>

Related Topics

[TLS Connections Details Table, on page 134](#)

TLS Connections Details Table

The TLS Connections Details table is an interactive table that shows the total number of connections, messages sent, and the number of TLS connections that are successful or failed, and the last TLS status for the incoming and outgoing messages. You can also view the percentage of successful and failed connections for each domain.

The following table shows the table column descriptions for the TLS Connection Details table:

Table 36: Table Column Descriptions for TLS Connections Details Table

Column Name	Description
Domain	The domain name of the sender.
TLS Req. Failed	All required TLS connections that failed.
TLS Req. Success	All required TLS connections that are successful.
TLS Pref. Failed	All preferred TLS connections that failed.
TLS Pref. Success	All preferred TLS connections that are successful.
Last TLS Status	The status of the TLS connections mapped based on the following: <ul style="list-style-type: none"> • 0: N/A • 1: Required - Fail • 2: Preferred - Fail • 3: Required - Success • 4: Preferred - Success
DANE Failure	Total number of unsuccessful outgoing TLS connections with DANE support.
DANE Success	Total number of successful outgoing TLS connections with DANE support.
Total TLS Connections	Total number of TLS connections.
Unencrypted Connections	Total number of unencrypted TLS connections.
% TLS of all Connections	The percentage of TLS encryptions for all TLS connections.
Messages by TLS	The total number of TLS messages.

Inbound SMTP Authentication Page

The Inbound SMTP Authentication report page shows the use of client certificates and the SMTP AUTH command to authenticate SMTP sessions between the Email Security appliance and users' mail clients. If the appliance accepts the certificate or SMTP AUTH command, it will establish a TLS connection to the mail client, which the client will use to send a message. Since it is not possible for the appliance to track these

attempts on a per-user basis, the report shows details on SMTP authentication based on the domain name and domain IP address.

Use this report to determine the following information:

- Overall, how many incoming connection use SMTP authentication?
- How many connections use a client certificated?
- How many connections use SMTP AUTH?
- What domains are failing to connect when attempting to use SMTP authentication?
- How many connections are successfully using the fall-back when SMTP authentication fails?

To view the Inbound SMTP Authentication report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Inbound SMTP Authentication** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The Inbound SMTP Authentication has two different views:

- Domains
- IP Addresses

These views provide a snapshot of the SMTP authentications in the context of the selected view.

The Inbound SMTP Authentication report page includes a graph for received connections, a graph for received recipients who attempted an SMTP authentication connection, and a table with details on the attempts to authenticate connections.

The following list explains the various sections on the Inbound SMTP Authentication report page:

Table 37: Details on the Inbound SMTP Authentication Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports , on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .
Received Connection Graph	The Received Connections graph shows the incoming connections from mail clients that attempt to authentication their connections using SMTP authentication over the time range you specify. The graph displays the total number of connections the appliance received, the number that did not attempt to authenticate using SMTP authentication, the number that failed and succeeded to authenticate the connection using a client certificate, and the number that failed and succeeded to authenticate using the SMTP AUTH command.

Section	Description
Received Recipient Graph	The Received Recipients graph displays the number of recipients whose mail clients attempted to authenticate their connections to the Email Security appliances to send messages using SMTP authentication. The graph also show the number of recipients whose connections were authenticated and the number of recipients whose connections were not authenticated.
SMTP Authentication Details (By Domain Name or IP Address).	The SMTP Authentication Details (by domain name and IP address) table displays details about the users who attempt to authenticate their connections to the Email Security appliance to send messages. For each domain, you can view the number of connection attempts using a client certificate that were successful or failed, the number of connection attempts using the SMTP AUTH command that were successful or failed, and the number that fell back to the SMTP AUTH after their client certificate connection attempt failed.

Rate Limits Page

Rate Limiting by envelope sender allows you to limit the number of email message recipients per time interval from an individual sender, based on the mail-from address. The Rate Limits report shows you the senders who most egregiously exceed this limit.

Use this report to help you identify the following:

- Compromised user accounts that might be used to send spam in bulk.
- Out-of-control applications in your organization that use email for notifications, alerts, automated statements, etc.
- Sources of heavy email activity in your organization, for internal billing or resource-management purposes.
- Sources of large-volume inbound email traffic that might not otherwise be considered spam.

To view the Rate Limits report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Rate Limits** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

Note that other reports that include statistics for internal senders (such as Internal Users or Outgoing Senders) measure only the number of messages sent; they do not identify senders of a few messages to a large number of recipients.

The Top Offenders by Incident chart shows the envelope senders who most frequently attempted to send messages to more recipients than the configured limit. Each attempt is one incident. This chart aggregates incident counts from all listeners.

The Top Offenders by Rejected Recipients chart shows the envelope senders who sent messages to the largest number of recipients above the configured limit. This chart aggregates recipient counts from all listeners.

Rate Limiting settings, including “Rate Limit for Envelope Senders” settings, are configured on the Email Security appliance in Mail Policies > Mail Flow Policies. For more information on rate limiting, see the documentation or online help for your Email Security appliance.

Related Topics

[High Volume Mail Page, on page 145](#)

Connections by Country Page

You can use the Connections by Country report page to view:

- Top incoming mail connections based on country of origin in graphical format.
- Total incoming mail connections and messages based on country of origin in tabular format.

To view the Connections by Country report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Connections by Country** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The following are the scenarios when no country information is displayed for the top and total incoming mail connections:

- The sender IP address belongs to a private IP address.
- The sender IP address does not get a valid SBRS.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

From the Connections by Country report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

Domain Protection Page

The Cisco Domain Protection cloud service interface automatically identifies, monitors and manages messages sent on your behalf. This provides an easy way to identify and eliminate illegitimate email messages and block malicious ones to prevent phishing attacks impersonating your company's domain. Domain Protection even detects the use of look-alike domains so the malicious URLs can be quickly taken down.

You can use the **Monitoring > Domain Protection** report page of the new web interface of your appliance to view:

- Summary of messages that are classified as legitimate or threat, in a graphical format.
- Summary of the destination domains details based on the senders, in a tabular format.

Make sure that you have a valid license to access Cisco Domain Protection cloud service interface with Administrator access privileges. To obtain a license, go to the Cisco Domain Protection registration page using the following URL: <https://www.cisco.com/c/en/us/buy.html>.

If you are already registered to Cisco Domain Protection, enter the following details to authenticate and view the Domain Protection reports on your appliance:

- **Client ID:** This is the API access UID used to import the reports from the Cisco Domain Protection cloud service.
- **Client Secret:** This is the API access key used to import the reports from the Cisco Domain Protection cloud service.

To generate API access UID and key, you must log in to the Cisco Domain Protection cloud service and go to **Settings > API Client Secret > Generate API Credentials**. For more information, see *User Guide for Cisco Domain Protection*.



Note To view the Domain Protection report page on the new web interface of your appliance, make sure that `trailblazerconfig` is enabled on your appliance.

User Mail Summary

The User Mail Summary report 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.

You can use the User Mail Summary report page to view:

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

To view the User Mail Summary report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > User Mail Summary** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

To search for specific information within your data, see [Searching and the Interactive Email Report Pages, on page 55](#).

The following list explains the various sections on the User Mail Summary report page:

Table 38: Details on the User Mail Summary Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports, on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .
Top Users by Clean Incoming Messages	The top users (by domain), of clean incoming messages received by your organization.
Top Users by Clean Outgoing Messages	The top users (by domain), of clean outgoing messages sent by your organization.

Section	Description
Top Users by Graymail	The top users (by domain), of graymail messages.
User Mail Flow Details	<p>The User Mail Flow Details interactive table breaks down the mails received and sent by each email address. You can sort the listing by clicking the column headers.</p> <p>For more information, see the User Mail Flow Details Table, on page 139.</p> <p>To view Message Tracking details for the messages that populate this report, click a blue number link in the table.</p>

From the User Mail Summary report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).



Note You can generate a scheduled report for the User Mail Summary page. See the [Scheduling Email Reports, on page 152](#).

Related Topics

- [User Mail Flow Details Table, on page 139](#)
- [Searching for a Specific Internal User, on page 74](#)

User Mail Flow Details Table

The User Mail Flow Detail table shows detailed information about a user, including a breakdown of incoming and outgoing messages, and the number of messages in each category (such as spam detected, virus detected, stopped by content filter, etc.). 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.

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

To view Message Tracking details for the messages that populate this report, click a number hyperlink in the table.

The following table shows the table column descriptions for the User Mail Flow Details table:

Table 39: Table Column Descriptions for User Mail Flow Details Table

Column Name	Description
Internal User	The domain name of the internal user.
Incoming Spam Detected	All incoming spam that was detected.
Incoming Virus Detected	The incoming virus that were detected.

Column Name	Description
Incoming Detected by Advanced Malware Protection	The incoming messages that are detected by Advanced Malware Protection (File Analysis and File Reputation).
Incoming Content Filter Matches	The incoming content filter matches that were detected.
Incoming Stopped by Content Filter	The incoming messages that were stopped due to content filters that have been set.
Incoming Marketing	The incoming messages that were detected as marketing.
Incoming Social Networking	The incoming messages that were detected as social networking.
Incoming Bulk	The incoming messages that were detected as bulk.
Incoming Graymails	The incoming messages that were detected as graymail.
Incoming Clean	All incoming clean messages.
Outgoing Spam Detected	The outgoing spam that was detected.
Outgoing Virus Detected	The outgoing viruses that were detected.
Outgoing Content Filter Matches	The outgoing content filter matches that were 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.

Searching for a Specific Internal User

With the search form at the bottom of the User Mail Summary page and the User Mail Flow Details 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”).

DLP Incident Summary Page

The DLP Incidents (DLP Incident Summary) report page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The Email Security 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?

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.

To view the DLP Incident Summary report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > DLP Incident Summary** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the DLP Incidents report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

To search for specific information within your data, see [Searching and the Interactive Email Report Pages , on page 55](#).

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

Table 40: Details on the DLP Incident Summary Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports , on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .
Top Incidents by Severity	The top DLP incidents listed by severity.
Incident Summary	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 DLP Incident Summary page. Click the name of a DLP policy to view more detailed information.
Top DLP Policy Matches	The top DLP Policies that have been matched.
DLP Incident Details	The DLP Incidents Details table shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages are delivered in the clear, delivered encrypted, or dropped. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

Web Interaction Page

You can use the Web Interaction report page to view:

- Top Malicious URLs clicked by End Users.

- Top Users who clicked on Rewritten Malicious URLs.
- Web Interaction Tracking Details.



Note Web Interaction report modules are populated only if the Web Interaction Tracking feature is enabled on managed Email Security appliances.

Web Interaction reports are available for incoming and outgoing messages. Only rewritten URLs (either by policy or Outbreak Filter) clicked by the end users are included in these modules.

To view the Web Interaction report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Web Interaction** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the Web Interaction report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

The following list explains the various sections on the Web Interaction report page:

Table 41: Details on the Web Interaction Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see Choosing a Time Range for Reports , on page 26 .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group, on page 25 .
Top Malicious URLs clicked by End Users	This section displays the summary of the top malicious URLs clicked by end users, for incoming and outgoing messages.
Top Users who clicked on Malicious URLs	This section displays the summary of the top end users who clicked on the Rewritten Malicious URLs, for incoming and outgoing messages.
Web Interaction Tracking Details	This section displays the chart view and the summary of malicious and neutral URLs of the incoming and outgoing messages. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

Web Interaction Tracking Details

The Web Interaction Tracking Details table is an interactive table which includes the following information:

- A list of all the rewritten URLs (malicious and unmalicious).
- Action taken (allow, block, or unknown) when a rewritten URL was clicked.

- If the verdict of a URL (clean or malicious) was unknown at the time when the end user clicked it, the status is shown as unknown. This could be because the URL was under further scrutiny or the web server was down or not reachable at the time of the user click.
- The number of times end users clicked on a rewritten URL.
- Note the following:
 - If you have configured a content or message filter to deliver messages after rewriting malicious URLs and notify another user (for example, an administrator), the web interaction tracking data for the original recipient is incremented if the notified user clicks on the rewritten URLs.
 - If you are sending a copy of quarantined messages containing rewritten URLs to a user other than the original recipient (for example, to an administrator) using the web interface, the web interaction tracking data for the original recipient is incremented if the other user clicks on the rewritten URLs.

To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

Remediation Reports Page

The Remediation Report page displays the remediation results of messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate.

On the Security Management appliance, click the **Monitoring** tab and select **Mail Flow Summary > User Reports > Remediation Report**.

You can use this report to:

- View the messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate.
- Know the reason for remediation failure. For example, connections errors, authentication errors, and so on.

The following list explains the various sections on the Remediation Report page:

Table 42: Details on the Remediation Reports Page

Section	Description
Summary	<p>The Summary section displays the following:</p> <ul style="list-style-type: none"> • Total number of messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate. • Number of messages successfully remediated for a configured remedial action. • Number of messages for which the remediation failed.

Section	Description
Mailbox Auto Remediation	<p>The Mailbox Auto Remediation report section displays the following:</p> <ul style="list-style-type: none"> • A list of recipients for whom the mailbox remediation was successful or unsuccessful. • Remedial actions taken on messages. • The filenames associated with a SHA-256 hash. Click the SHA-256 hash to view the related messages in the Message Tracking page. • A list of profile names defined for the recipients for whom the mailbox remediation was successful or unsuccessful. • Reason for the remediation failure. <p>Note After upgrading to AsyncOS 13.6.1, the message tracking status of the messages received before the upgrade remains as "Delivered" than "Remediated."</p>
Mailbox Search and Remediate	<p>The Mailbox Search and Remediate section displays the following details:</p> <ul style="list-style-type: none"> • The list of remediation batches that are in progress or completed. • The remediation status of the messages in the batches. • The batch name and batch ID. Click the batch name to view the batch details: <ul style="list-style-type: none"> • The date and time when the remediation was initiated. • The source from which the remediation was initiated. • The host who initiated the remediation of the messages. • The remedial action taken on the messages. • The Cisco Ironport Message ID of the message. • A read receipt icon to show if the message was read by the recipient before the message was remediated successfully. • The remediation status of the message in the particular batch as Success, Failed, or In Progress. • The email address of the sender who sent the message. • The email addresses of the recipients for whom the message was delivered and later attempted for remediation. • The date and time when the message was sent to the recipient.

Message Filters Page

The Message Filters report page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages.

You can use the Message Filters report page to view:

- Top message filter by number of matches in graphical format.
- Total message filter by number of matches in tabular format.

To view the Message Filters report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Message Filters** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the Message Filters report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

High Volume Mail Page

You can use the High Volume Mail report page to:

- Identify attacks involving a large number of messages from a single sender, or with identical subjects, within a moving one-hour period.
- Monitor top domains to ensure that such attacks do not originate in your own domain. If this situation occurs, one or more accounts in your organization may be compromised.
- Help identify false positives so you can adjust your filters accordingly.

You can use the High Volume Mail report page to view:

- Messages with the top subjects in graphical format.
- Messages with the top envelope senders in graphical format.
- Top message filters by number of matches in graphical format.
- Total message filters by number of matches in tabular format.

To view the High Volume Mail report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > High Volume Mail** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the High Volume Mail report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).

Reports on this page show data only from message filters that use the Header Repeats rule and that pass the number-of-messages threshold that you set in that rule. When combined with other rules, the Header Repeats rule is evaluated last, and is not evaluated at all if the message disposition is determined by a preceding condition. Similarly, messages caught by Rate Limiting never reach Header Repeats message filters. Therefore, some messages that might otherwise be considered high-volume mail may not be included in these reports. If you have configured your filters to include certain messages in allowed list, those messages are also excluded from these reports.

For more information about message filters and the Header Repeats rule, see the online help or user guide for your Email Security appliance.

Content Filters Page

The Content Filters report 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 report page, you can 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?

You can use the Content Filter report page to view:

- Top incoming and outgoing content filter matches in graphical format.
- Top incoming and outgoing content filter matches in tabular format.

To view the Content Filters report page on the Security Management appliance, select **Email** from the Product drop-down and choose **Monitoring > Content Filters** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the Content Filters report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Exporting Reporting and Tracking Data , on page 31](#).



Note Note You can generate a scheduled report for the Content Filter page. See the [Scheduling Email Reports, on page 152](#).

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 [User Mail Summary, on page 138](#).

If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

Reporting Data Availability Page

From the Reports drop-down, select **Monitoring > Reporting Data Availability** on the new web interface of your appliance to view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.

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.

Reporting of Graymail

Graymail statistics are reflected in the following reports:

Report	Contains the Following Graymail Data
Mail Flow Summary page > Incoming tab	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages.
Mail Flow Details page > Outgoing Senders tab	The top graymail senders.
Mail Flow Details page > Incoming Mails tab	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for all the IP addresses, domain names, or network owners.
User Mail Summary page > Top Users by Graymail	The top end users who receive graymail.
User Mail Summary page > User Mail Details	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for all the users.

Related Topics

- [Reporting of Marketing Messages after Upgrade to AsyncOS 9.5](#), on page 91

Reporting of Marketing Messages after Upgrade to AsyncOS 9.5

After upgrade to AsyncOS 9.5:

- The number of marketing messages is the sum of marketing messages detected before and after the upgrade.
- The total number of graymail messages does not include the number of marketing messages detected before the upgrade.
- The total number of attempted messages also includes the number of marketing messages detected before the upgrade.
- If the graymail feature is not enabled on managed Email Security appliances, marketing messages are counted as clean messages.

About Scheduled and On-Demand Email Reports

Types of Reports Available

Except as noted, the following types of Email Security reports are available as both 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, on page 146](#).
- DLP Incident Summary—For information on what is included on this page, see the [DLP Incident Summary Page, on page 140](#).

- **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 documentation or online help for your Email Security appliance.
- **Domain-Based Executive Summary**—This report is based on the [Mail Flow Summary Page, on page 100](#), and is limited to a group of specified domains. For information on what is included, see the [Domain-Based Executive Summary Report, on page 149](#).
- **Executive Summary**—This report is based on the information from the [Mail Flow Summary Page, on page 100](#). For information on what is included, see the [Domain-Based Executive Summary Report, on page 149](#).
- **Mail Flow Details** — For information on what is included on this page, see the [Mail Flow Details Page, on page 122](#).
- **User Mail Summary**—For information on what is included on this page, see the [User Mail Summary, on page 138](#).
- **Outgoing Destinations**—For information on what is included on this page, see the [Outgoing Destinations Page, on page 130](#).
- **Sender Groups** —For information on what is included on this page, see the [Sender Groups Page, on page 129](#).
- **TLS Encryptions**—For information on what is included on this page, see the [TLS Encryption Page, on page 132](#).
- **Virus Types**—For information on what is included on this page, see the [Virus Filtering Page, on page 114](#).

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 report or export raw data as a CSV file 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 [Exporting Reporting and Tracking Data , on page 31](#).

Storage of Archived Reports

For information on how long reports are stored for, and when archived reports are deleted from the system, see [Viewing and Managing Archived Email Reports , on page 155](#).

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, on page 149](#)
- [Executive Summary Report, on page 151](#)

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. The outgoing mail summary shows data only when the domain in the PTR (pointer record) of the sending server matches a domain you specify. If multiple domains are specified, the appliance aggregates the data for all those domains into a single report.

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.

Unlike other scheduled reports, Domain-Based Executive Summary reports are not archived.

Domain-Based Executive Summary Reports and Messages Blocked by Sender Reputation Filtering

Because messages blocked by sender 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 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 Email Security appliance. However, this option can impact system performance. For more information about delayed HAT rejections, see the documentation for your Email Security appliance.



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.

Managing Lists of Domains and Recipients for Domain-Based Executive Summary Reports

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.

Creating Domain-Based Executive Summary Reports

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

To schedule the report:

- a) [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- b) Choose **Email > Reporting > Scheduled Reports**.
- c) Click **Add Scheduled Report**.

To create an on-demand report:

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

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

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 [Managing Lists of Domains and Recipients for Domain-Based Executive Summary Reports](#), on page 149.

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 allowed list 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 raw 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 logo is used.
- Step 10** Select a language for this report. For generating PDFs in Asian languages, see important information at [Exporting Reporting and Tracking Data](#), on page 31.
- Step 11** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
-

Executive Summary Report

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 [Mail Flow Summary Page](#), on page 100. For more information on the Email Reporting Overview page, see [Mail Flow Summary Page](#), on page 100.

Scheduled Reports Page

- [Scheduling Email Reports](#), on page 152
- [Scheduling Web Reports](#), on page 221

Scheduling Email Reports

You can schedule any of the reports listed in [About Scheduled and On-Demand Email Reports](#) , on page 147.

To manage report scheduling, see the following:

- [Adding Scheduled Reports](#), on page 152
- [Editing Scheduled Reports](#), on page 153
- [Discontinuing Scheduled Reports](#) , on page 153

My Email Report is a user report under the Scheduled Reports menu. The user reports can only be seen by the user who has created them.



Note The scheduled reports of the legacy web interface are not displayed under the **Scheduled Reports** tab of the new web interface. The scheduled reports of the new web interface are not displayed on the **Scheduled Reports** page of the legacy web interface.

Adding Scheduled Reports

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

Step 1 Choose **Email > Reporting > Scheduled Reports**.

Step 2 Click **Add Scheduled Report**.

Step 3 Choose your report type.

For descriptions of the report types, see [About Scheduled and On-Demand Email Reports](#) , on page 147.

Note - For information about the settings for a Domain-Based Executive Summary report, see [Domain-Based Executive Summary Report](#), on page 149.

- 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.

Step 6 Choose the format for the generated report.

The default format is PDF. Most reports also allow you to save raw data as a CSV file.

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 [Exporting Reporting and Tracking Data](#) , on page 31.

Step 12 Click **Submit**.

Editing Scheduled Reports

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Email > Reporting > Scheduled Reports**.


Step 3 Click the report name link in the Report Title column that you want to modify.

Step 4 Modify the report settings.

Step 5 Submit and commit your changes.

Discontinuing Scheduled Reports

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

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Email > Reporting > Scheduled Reports**.

Step 3 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 4 Click **Delete**.

Note Any archived versions of deleted reports are *not* automatically deleted. To delete previously-generated reports, see [Deleting Archived Reports](#), on page 155.

Generating Email 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 on the New Web Interface](#), on page 95, you can save PDFs or raw-data CSV files for the reports listed in [About Scheduled and On-Demand Email Reports](#) , on page 147 at any time, for the time frame that you specify.

To generate an on-demand report perform the following:

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Email > Reporting > Archived Reports**.
- Step 3** Click **Generate Report Now**.
- Step 4** Choose a report type.
- For descriptions of the report types, see [About Scheduled and On-Demand Email Reports](#) , on page 147.
- Step 5** 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](#), on page 149.
- 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 6** From the Time Range to Include drop-down list, select a time range for the report data.
- Note the custom time range option.
- 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 raw 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** 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 9** 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 10** Select a language for this report. For generating PDFs in Asian languages, see important information at [Exporting Reporting and Tracking Data](#) , on page 31.
- Step 11** Click **Deliver This Report** to generate the report.
-

Archived Email Reports Page

- [About Scheduled and On-Demand Email Reports](#) , on page 147
- [Generating Email Reports On Demand](#) , on page 153
- [Viewing and Managing Archived Email Reports](#) , on page 155

Viewing and Managing Archived Email Reports

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 30 instances of each scheduled report, up to 1000 total versions for all reports. The limit of 30 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 [IP Interfaces and Accessing the Appliance](#), on page 609 for more information.)


My Email Reports under the Archive reports can only be seen by the user who created the Scheduled report.



Note The archived reports of the legacy web interface are displayed under the **View Legacy Archived Reports** tab of the new web interface. The archived reports of the new web interface are not displayed on the legacy web interface.

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.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 2** Choose **Email > Reporting > Archived Reports**.
 - Step 3** 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 4** Click the Report Title to view that report.
-

Deleting Archived Reports

Reports are automatically deleted from the system according to the rules outlined in [Viewing and Managing Archived Email Reports](#) , on page 155. However, you can manually delete unneeded reports.

To manually delete Archived reports, perform the following:

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Email > Reporting > Archived Reports**.
The Archived reports that are available are displayed.
- Step 3** Select the checkbox for one or more reports to delete.
- Step 4** Click **Delete**.
- Step 5** To prevent future instances of scheduled reports from being generated, see [Discontinuing Scheduled Reports](#), on page 153.
-

Scheduling and Archiving Email Reports on the New Web Interface

My Email Report is a user report under the Scheduled Reports menu. The user reports can only be seen by the user who has created them. My Email Reports under the Archive reports can only be seen by the user who created the Scheduled report.

- [Scheduling Email Reports on the New Web Interface, on page 156](#)
- [Archived Email Reports Page on the New Web Interface, on page 158](#)



Note The scheduled reports of the legacy web interface are not displayed under the **Scheduled Reports** tab of the new web interface. The scheduled reports of the new web interface are not displayed on the **Scheduled Reports** page of the legacy web interface.

The archived reports of the legacy web interface are displayed under the **View Legacy Archived Reports** tab of the new web interface. The archived reports of the new web interface are not displayed on the legacy web interface.

Scheduling Email Reports on the New Web Interface

- [Adding Scheduled Reports on the New Web Interface, on page 156](#)
- [Editing Scheduled Reports on the New Web Interface, on page 157](#)
- [Discontinuing Scheduled Reports on the New Web Interface, on page 158](#)

Adding Scheduled Reports on the New Web Interface




Note You can schedule your favorite reports (My Email Reports) page. For information on how to add schedule reports, see [Scheduling Email Reports on the New Web Interface](#).

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

-
- Step 1** Log in to the new web interface of the appliance.
- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** In the **Schedule Reports** tab, click the + button.
- Step 4** Choose your report type.
- For descriptions of the report types, see [About Scheduled and On-Demand Email Reports](#) , on page 147.
- Note** - For information about the settings for a Domain-Based Executive Summary report, see [Domain-Based Executive Summary Report](#), on page 149.
- 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** 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 6** Choose the time range for the report from the **Time Range to Include** drop-down menu.
- Step 7** Choose the format for the generated report.
- The default format is PDF.
- Note** You can export My Favorite Reports page or download My Favorite Reports page as a PDF. For more information, see [Exporting Reporting and Tracking Data](#) .
- Step 8** From the **Email Appliance(s)** section, select the Email Security appliance from the drop-down list.
- Step 9** From the Delivery Options section, choose any one of the following:
- By choosing this, the report will be listed on the Archived Reports page.
- Note** Domain-Based Executive Summary reports cannot be archived.
- To archive the report, select **Only Archive**.
 - To archive and email the report, click **Archive and Email to Recipients**.
 - To email the report, click **Only Email to Recipients**.
- In the **Email IDs** field, enter the recipient email addresses.
- Step 10** From the **Scheduling** section, 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 11** Choose a language for the report.
- Step 12** Click **Submit**.
-

Editing Scheduled Reports on the New Web Interface

- Step 1** Log in to the new web interface of the appliance.

- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** In the Schedule Reports tab, select the check box next to the required Report Title column and click the  button.
- Step 4** Modify the report settings.
- Step 5** Submit and commit your changes.

Discontinuing Scheduled Reports on the New Web Interface

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

- Step 1** Log in to the new web interface of the appliance.
- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** In the Schedule Reports tab, 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 4** Click **Delete**.
- Note** Any archived versions of deleted reports are *not* automatically deleted. To delete previously-generated reports, see [Accessing Archived Reports on the New Web Interface, on page 158](#).

Archived Email Reports Page on the New Web Interface

- [Accessing Archived Reports on the New Web Interface, on page 158](#)
- [Generating Email Reports On Demand, on page 159](#)
- [Deleting Archived Reports on the New Web Interface, on page 160](#)

Accessing Archived Reports on the New Web Interface

The **View Archived Reports** tab of the **Schedule & Archive** page lists scheduled and on-demand reports that you have chosen to archive which have been generated and not yet purged.



- Note** You can archive your favorite reports (My Email Reports) page. For information on how to add archive reports, see [Archived Email Reports Page on the New Web Interface](#).

- Step 1** Log in to the new web interface of the appliance.
- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** Click on the **View Archived Reports** tab.
- Step 4** To locate a particular report if the list is long, you can search for the report name and type or click a column heading to sort by that column.

Generating Email 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 on the New Web Interface, on page 95](#), you can save PDFs or raw-data CSV files for the reports listed in [About Scheduled and On-Demand Email Reports , on page 147](#) at any time, for the time frame that you specify.

To generate an on-demand report perform the following:

-
- Step 1** Log in to the new web interface of the appliance.
- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** In the View Archived Reports tab, click on the + button.
- Step 4** Choose a report type.
- For descriptions of the report types, see [About Scheduled and On-Demand Email Reports , on page 147](#).
- Step 5** In the **Title** field, enter 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, on page 149](#).
- 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 6** From the **Time Range to Include** drop-down list, select a time range for the report data.
- Note the custom time range option.
- 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 raw 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** 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 9** From the Email Appliance(s) section, select the Email Security appliance from the drop-down list.
- Step 10** From the Delivery Options section, choose any one of the following:
- By choosing this, the report will be listed on the Archived Reports page.
- Note** Domain-Based Executive Summary reports cannot be archived.
- To archive the report, select **Only Archive**.
 - To archive and email the report, click **Archive and Email to Recipients**.
 - To email the report, click **Only Email to Recipients**.

In the **Email IDs** field, enter the recipient email addresses.

- Step 11** Select a language for this report. For generating PDFs in Asian languages, see important information at [Exporting Reporting and Tracking Data](#), on page 31.
- Step 12** Click **Submit** to generate the report.

Deleting Archived Reports on the New Web Interface

Reports are automatically deleted from the system according to the rules outlined in [Viewing and Managing Archived Email Reports](#), on page 155. However, you can manually delete unneeded reports.

To manually delete Archived reports, perform the following:

- Step 1** Log in to the new web interface of the appliance.
- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** In the View Archived Reports tab, select the checkbox for one or more reports to delete.
- Step 4** Click on the trash can button.
- Step 5** To prevent future instances of scheduled reports from being generated, see [Discontinuing Scheduled Reports on the New Web Interface](#), on page 158.

Troubleshooting Email Reports

- [Outbreak Filters Reports Do Not Show Information Correctly](#), on page 160
- [Message Tracking Results Do Not Match Report Results After Clicking a Link in a Report](#), on page 160
- [Advanced Malware Protection Verdict Updates Report Results Differ](#), on page 161
- [Issues Viewing File Analysis Report Details](#), on page 161

See also [Troubleshooting All Reports](#), on page 33.

Outbreak Filters Reports Do Not Show Information Correctly

Problem

Outbreak Filters reports do not show threat information correctly.

Solution

Verify that the appliance can communicate with the Cisco update servers specified in Management Appliance > System Administration > Update Settings.

Message Tracking Results Do Not Match Report Results After Clicking a Link in a Report

Problem

Message tracking results when drilling down from reports do not match expected results.

Solution

This can occur if reporting and tracking are not consistently and simultaneously enabled and functioning properly, or are not consistently and simultaneously either centralized or stored locally on each Email Security appliance. Data for each feature (reporting, tracking) is captured only while that feature is enabled.

Related Topics

- [Checking Message Tracking Data Availability](#) , on page 253

Advanced Malware Protection Verdict Updates Report Results Differ

Problem

A Web Security appliance and an Email Security appliance sent the same file for analysis, and the AMP Verdict Updates reports for Web and Email show different verdicts for that file.

Solution

This situation is temporary. Results will match once all verdict updates have been downloaded. Allow up to 30 minutes for this to occur.

Issues Viewing File Analysis Report Details

- [File Analysis Report Details Are Not Available](#) , on page 161
- [Error When Viewing File Analysis Report Details](#), on page 161
- [Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance](#) , on page 161
- [Logging of File Analysis-Related Errors](#) , on page 162

File Analysis Report Details Are Not Available

Problem

File Analysis report details are not available.

Solution

See [Requirements for File Analysis Report Details](#) , on page 82.

Error When Viewing File Analysis Report Details

Problem

No cloud server configuration is available error appears when you attempt to view File Analysis report details.

Solution

Go to **Management Appliance > Centralized Services > Security Appliances** and add at least one Email Security appliance that has the File Analysis feature enabled.

Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance

Problem

You see an API key, registration, or activation error when attempting to view File Analysis report details.

Solution

If you are using a private cloud (on-premises) Cisco AMP Threat Grid appliance for file analysis, see [\(On-Premises File Analysis\) Activate the File Analysis Account , on page 83](#).

If your Threat Grid appliance hostname changes, you must repeat the process in the referenced procedure.

Logging of File Analysis-Related Errors

Registration and other File Analysis-related errors are logged in the GUI logs.

Total Graymail or Marketing Messages Appears To Be Incorrect

Problem

The count of Marketing, Social and Bulk mail exceeds the total number of graymail messages.

Solution

The total number of Marketing Messages includes marketing messages received both before and after upgrade to AsyncOS 9.5, but the total number of graymail messages includes only messages received after upgrade. See [Reporting of Marketing Messages after Upgrade to AsyncOS 9.5 , on page 91](#).



CHAPTER 6

Using Centralized Web Reporting and Tracking

This chapter contains the following sections:

- [Centralized Web Reporting and Tracking Overview](#), on page 163
- [Setting Up Centralized Web Reporting and Tracking](#), on page 165
- [Working with Web Security Reports](#), on page 167
- [Working with Web Security Reports on the New Web Interface](#), on page 167
- [Web Reporting Page Descriptions](#), on page 168
- [Understanding the Web Reporting Pages on the New Web Interface](#), on page 195
- [About Scheduled and On-Demand Web Reports](#), on page 220
- [Scheduling Web Reports](#), on page 221
- [Generating Web Reports on Demand](#), on page 224
- [Archived Web Reports Page](#), on page 225
- [Viewing and Managing Archived Web Reports](#), on page 226
- [Schedule and Archive Web Reports on the New Web Interface](#), on page 226
- [Web Tracking](#), on page 229
- [Web Tracking on the New Web Interface](#), on page 234
- [Working with Web Tracking Search Results](#), on page 239
- [Troubleshooting Web Reporting and Tracking](#), on page 241

Centralized Web Reporting and Tracking Overview

The Cisco Secure Email and Web Manager appliance aggregates information from security features on multiple Web Security appliances 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 URL category.

Domain

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

URL Category

For a URL 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.

General

For a detailed description on logging pages versus reporting pages, see the [Logging Versus Reporting, on page 565](#).



Note You can 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 [Searching for Transactions Processed by Web Proxy Services, on page 229](#) on the Web Tracking page.



Note 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 retains ONLY System Capacity and System Status data. If Centralized Web Reporting is not enabled, the only reports that are generated are System Status and System Capacity.

There are multiple ways to view web reporting data on the Security Management appliance.


- To view interactive report pages, see [Web Reporting Page Descriptions, on page 168](#).
- To generate a report on demand, see [Generating Web Reports on Demand, on page 224](#).
- To schedule generation of reports on a regular, recurring basis, see [About Scheduled and On-Demand Web Reports, on page 220](#).
- To view archived versions of previously run reports (both scheduled and generated on demand), see [Viewing and Managing Archived Web Reports, on page 226](#).
- To view information about individual transactions, see [Web Tracking, on page 229](#).

Setting Up Centralized Web Reporting and Tracking

To set up centralized web reporting and tracking, complete the following steps in order:

- [Enabling Centralized Web Reporting on the Security Management Appliance](#) , on page 165
 - [Anonymizing User Names in Web Reports](#) , on page 166
- [Enabling Centralized Web Reporting on Web Security Appliances](#) , on page 165
- [Adding the Centralized Web Reporting Service to Each Managed Web Security Appliance](#) , on page 165
- [Anonymizing User Names in Web Reports](#) , on page 166

Enabling Centralized Web Reporting on the Security Management Appliance

-
- Step 1** Before enabling centralized web reporting, ensure that sufficient disk space is allocated to that service. See [Managing Disk Space](#) , on page 521.
- Step 2** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 3** Choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.
- Step 4** If you are enabling centralized reporting for the first time after running the System Setup Wizard:
- a) Click **Enable**.
 - b) Review the end user license agreement, then click **Accept**.
- Step 5** If you are enabling centralized reporting after it has previously been disabled:
- a) Click **Edit Settings**.
 - b) Select the **Enable Centralized Web Report Services** checkbox.
 - c) You can address [Anonymizing User Names in Web Reports](#) , on page 166 now or later.
- Step 6** Submit and commit your changes.
-

Enabling Centralized Web Reporting on Web Security Appliances


All Web Security appliances should be configured and working as expected before you enable centralized reporting.

You must enable centralized reporting on each Web Security appliance that will use centralized reporting.

See the “Enabling Centralized Reporting” section in AsyncOS for Cisco Web Security Appliances User Guide.

Adding the Centralized Web Reporting Service to Each Managed Web Security Appliance

The steps you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.


-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** If you have already added the Web Security appliance to the list:
- Click the name of a Web Security Appliance.
 - Select the **Centralized Reporting** service.
- Step 4** If you have not yet added Web Security appliances:
- Click Add Web Appliance.
 - In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Web Security 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**.
- The Centralized Reporting service is pre-selected.
 - Click **Establish Connection**.
 - Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.
- 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.
- Wait for the Success message to appear above the table on the page.
 - Click **Test Connection**.
 - Read test results above the table.
- Step 5** Click **Submit**.
- Step 6** Repeat this procedure for each Web Security Appliance for which you want to enable Centralized Reporting.
- Step 7** Commit your changes.
-

Anonymizing User Names in Web Reports

By default, user names appear on reporting pages and PDFs. However, to protect user privacy, you may want to make user names unrecognizable in web reports.



Note Users with Administrator privileges on this appliance can always see user names when viewing interactive reports.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.
- Step 3** Click **Edit Settings**.
- Step 4** Select the **Anonymize usernames in reports** checkbox.

Step 5 Submit and commit your change.

Working with Web Security Reports

Web reporting pages allow you to monitor information on one or all of the managed Web Security appliances in your system.

To	See
View options for accessing and viewing report data	Ways to View Reporting Data , on page 23
Customize your view of the interactive report pages	Customizing Your View of Report Data , on page 25
Find information about specific transactions within your data	Web Tracking , on page 229
Print or export report information	Exporting Reporting and Tracking Data , on page 31
Understand the various interactive report pages	Web Reporting Page Descriptions , on page 168
Generate a report on demand	Understanding the Web Reporting Pages on the New Web Interface , on page 195
Schedule reports to run automatically at intervals and times that you specify	About Scheduled and On-Demand Web Reports , on page 220
View archived on-demand and scheduled reports	Viewing and Managing Archived Web Reports , on page 226
Understand how data is gathered	How the Security Management Appliance Gathers Data for Reports , on page 24

Working with Web Security Reports on the New Web Interface

Web reporting pages allow you to monitor information on one or all of the managed Web Security appliances in your system.

To	See
View options for accessing and viewing report data	Ways to View Reporting Data , on page 35
Customize your view of the interactive report pages	Customizing Your View of Report Data , on page 38
Find information about specific transactions within your data	Web Tracking on the New Web Interface , on page 234
Print or export report information	Exporting Reporting and Tracking Data , on page 31

To	See
Understand the various interactive report pages	Understanding the Web Reporting Pages on the New Web Interface, on page 195

Web Reporting Page Descriptions



Note For information on which of the options on the Web Reporting tab are available as on-demand or scheduled reports, see the [About Scheduled and On-Demand Web Reports, on page 220](#).

Table 43: Web Reporting Tab Details

Web Reporting Menu	Action
Web Reporting Overview , on page 171	The Overview page provides a synopsis of the activity on your Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the Web Reporting Overview , on page 171 .
Users Report (Web) , on page 172	<p>The Users page provides several web tracking links that allow you to view web tracking information for individual users.</p> <p>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.</p> <p>From the Users 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 User Details page allows you to see specific information about a user that you have identified in the Users table on the Web > Reporting > Users 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 Users Report (Web) , on page 172. For information on a specific user in your system, see the User Details (Web Reporting) , on page 173</p>
User Count Report (Web)	<p>The User Count page provides the aggregated information about the total number of authenticated and unauthenticated users of the Web Security appliances with Centralized Reporting enabled. The page lists the unique user count for the last 30 days, 90 days, and 180 days.</p> <p>Note System hourly computes the total user count of authenticated and unauthenticated users.</p>

Web Reporting Menu	Action
Web Sites Report , on page 175	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 Web Sites Report , on page 175.
URL Categories Report , on page 176	The URL Categories page allows you to view the top URL Categories that are being visited, including: <ul style="list-style-type: none"> • the top URLs that have triggered a block or warning action to occur per transaction. • 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. For more information, see the URL Categories Report , on page 176.
Application Visibility Report , on page 178	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 Application Visibility Report , on page 178.
Anti-Malware Report , on page 180	The Anti-Malware page allows you to view information about malware ports and malware sites that the anti-malware scanning engine(s) 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 Anti-Malware Report , on page 180.
Advanced Malware Protection (File Reputation and File Analysis) Reports , on page 182	There are three reporting pages showing file reputation and analysis data. For more information, see the Advanced Malware Protection (File Reputation and File Analysis) Reports , on page 182.
Client Malware Risk Report , on page 187	The Client Malware Risk page is a security-related reporting page that can be used to identify individual client computers that may be connecting unusually frequently to malware sites. For more information, see the Client Malware Risk Report , on page 187.
Web Reputation Filters Report , on page 188	Allows you to view reporting on Web Reputation filtering for transactions during a specified time range. For more information, see the Web Reputation Filters Report , on page 188.
L4 Traffic Monitor Report , on page 189	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 L4 Traffic Monitor Report , on page 189.
SOCKS Proxy Report , on page 191	Allows you to view data for SOCKS proxy transactions, including destinations and users. For more information, see the SOCKS Proxy Report , on page 191.

Web Reporting Menu	Action
Reports by User Location , on page 191	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. For more information, see the Reports by User Location , on page 191.
Web Tracking , on page 229	The Web Tracking page allows you to search for the following types of information: <ul style="list-style-type: none"> • Searching for Transactions Processed by Web Proxy Services , on page 229 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>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> <ul style="list-style-type: none"> • Searching for Transactions Processed by the L4 Traffic Monitor , on page 233 allows you to search your L4TM data for sites, ports, and client IP addresses involved in malware transfer activity. • Searching for Transactions Processed by the SOCKS Proxy , on page 234 allows you to search for transactions processed by the SOCKS proxy. <p>For more information, see the Web Tracking , on page 229.</p>
System Capacity Page , on page 192	Allows you to view the overall workload that is sending reporting data to the Security Management appliance. For more information, see the System Capacity Page , on page 192.
Data Availability Page , on page 194	Allows you to get a glimpse of the impact of the reporting data on the Security Management appliance for each appliance. For more information, see the Data Availability Page , on page 194.
Scheduled Reports	Allows you to schedule reports for a specified time range. For more information, see the About Scheduled and On-Demand Web Reports , on page 220.
Archived Reports	Allows you to archive reports for a specified time range. For more information, see the Viewing and Managing Archived Web Reports , on page 226.



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 [About Scheduled and On-Demand Web Reports](#), on page 220.

About Time Spent

The Time Spent column in various tables represents the amount of time a user 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.

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.

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.

For the purposes of the time spent value, considering the following notes:

- An active user is defined as a user name or IP address that sends HTTP traffic through the appliance and has gone to a website that AsyncOS considers to be a “page view.”
- 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.

Units are displayed in Hours:Minutes format.

Web Reporting Overview

The **Web > Reporting > Overview** page provides a synopsis of the activity on your Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions.

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.

Table 44: Details on the Web Reporting Overview 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 Choosing a Time Range for Reports , on page 26.
View Data for	Choose a Web Security appliance for which you want to view Overview data, or choose All Web Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group , on page 25.
Total Web Proxy Activity	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. This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).
Web Proxy Summary	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.
L4 Traffic Monitor Summary	This section reports any L4 traffic that is being reported by the Web Security appliances that are currently managed by the Security Management appliance.

Section	Description
Suspect Transactions	This section allows you to view the web transactions that have been labeled as suspect by the administrator. This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).
Suspect Transactions Summary	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.
Top URL Categories by Total Transactions	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). The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 177.
Top Application Types by Total Transactions	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).
Top Malware Categories Detected	This section displays all Malware categories that have been detected.
Top Users Blocked or Warned Transactions	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. To make user names unrecognizable, see Anonymizing User Names in Web Reports , on page 166.
Web Traffic Tap Status	Displays the untapped and tapped traffic transactions in a graph format.
Web Traffic Tap Summary	Displays the summary of the tapped and untapped traffic transactions along with the total traffic transactions.
Tapped HTTP/HTTPS Traffic	Displays the tapped HTTP and HTTPS traffic transactions in a graph format.
Tapped Traffic Summary	Displays the summary of HTTP and HTTPS traffic transactions along with the total HTTP/HTTPS traffic transactions.

Users Report (Web)

The **Web > Reporting > Users** page provides several links that allow 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.

From the **Users** page, you can view the following information pertaining to the users on your system:

Table 45: 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 Choosing a Time Range for Reports , on page 26.
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 Enabling Centralized Web Reporting on the Security Management Appliance , on page 165. The default setting is that all user names appear. To hide user names, see Anonymizing User Names in Web Reports , on page 166.
Top Users by Bandwidth Used	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).
Users Table	<p>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 Find User ID or Client IP Address. 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 User Details (Web Reporting) , on page 173</p>



Note To view user IDs instead of client IP addresses, you must set up your Security Management appliance to obtain user information from an LDAP server. For information, see [Creating the LDAP Server Profile](#), on page 372 in chapter [Integrating With LDAP](#), on page 371.



Tip To customize your view of this report, see [Working with Web Security Reports](#), on page 167.

To view an example of how the **Users** page may be used, see [Example 1: Investigating a User](#) , on page 625.



Note You can generate or schedule a report for the Users page. For information, see the [About Scheduled and On-Demand Web Reports](#), on page 220.

User Details (Web Reporting)

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.

From the **User Details** page, you can view the following information pertaining to an individual user on your system:

Table 46: Details on the Web Reporting User Details Page

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports , on page 26.
URL Categories by Total Transactions	This section lists the specific URL Categories that a specific user is using. The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 177.
Trend by Total Transactions	This graph displays at what times the user accessed the web. 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.
URL Categories Matched	The URL Categories Matched section shows matched categories for both completed and blocked transactions. 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 Find URL Category . The category does not need to be an exact match. The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 177.
Domains Matched	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 Find Domain or IP . The domain or IP address does not need to be an exact match.
Applications Matched	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. In the text field at the bottom of the section enter the application name and click Find Application . The name of the application does not need to be an exact match.
Malware Threats Detected	From this table you can see the top Malware threats that a specific user is triggering. You can search for data on a specific malware threat name in the Find Malware Threat field. Enter the Malware Threat name and click Find Malware Threat. The name of the Malware Threat does not need to be an exact match.
Policies Matched	From this section you can find the policy groups that applied to this user when accessing the web. In the text field at the bottom of the section enter the policy name and click Find Policy . The name of the policy does not need to be an exact match.



Note From Client Malware Risk Details table: 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.

To view an example of how the User Details page may be used, see [Example 1: Investigating a User](#), on page 625.

User Count Report (Web)

The **Web > Reporting > User Count** page displays the aggregated information about the total number of authenticated and unauthenticated users of the Web Security appliances with Centralized Reporting enabled. The page lists the unique user count for the last 30 days, 90 days, and 180 days.



Note System hourly computes the total user count of authenticated and unauthenticated users.

Web Sites Report

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.

From the **Web Sites** page, you can view the following information:

Table 47: 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 Choosing a Time Range for Reports , on page 26.
Top Domains by Total Transactions	This section lists the top domains that are being visited on the site in a graph format.
Top Domains by Transactions Blocked	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 is listed in this graph as a transaction blocked, and the domain site that triggered the block action is listed.

Section	Description
Domains Matched	<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 Proxy Services tab on the Web Tracking page appears and you can see tracking information and why certain domains were blocked.</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.</p> <p>To view an example of how Web Tracking may be used, see Example 2: Tracking a URL, on page 627.</p> <p>Note If you export this data to a .csv file, only the first 300,000 entries are exported.</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).



Note You can generate or schedule a report for information on the Web Sites page. For information, see the [About Scheduled and On-Demand Web Reports, on page 220](#).

URL Categories Report

The **Web > Reporting > URL Categories** page can be used to view the URL categories of sites that users on your system are visiting.

From the **URL Categories** page, you can view the following information:

Table 48: Details on the Web Reporting URL Categories Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26 .
Top URL Categories by Total Transactions	This section lists the top URL Categories that are being visited on the site in a graph format.
Top URL Categories by Blocked and Warned Transactions	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.
URL Categories Matched	<p>The URL Categories Matched section shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category.</p> <p>If there are a large number of unclassified URLs, see Reducing Uncategorized URLs , on page 177.</p>

Section	Description
URL Filtering Bypassed	Represents policy, port, and admin user agent blocking that occurs before URL filtering.



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).



Note To generate a more detailed report than this page can provide, see [Top URL Categories—Extended, on page 223](#).

- 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.

Reducing Uncategorized URLs

If the percentage of uncategorized URLs is higher than 15-20%, consider the following options:

- For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. These transactions will then be included in “URL Filtering Bypassed” statistics instead. To do this, see information about custom URL categories AsyncOS for Cisco Web Security Appliances User Guide.
- For sites that you feel should be included in existing or other categories, see [Reporting Misclassified and Uncategorized URLs , on page 178](#).

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated on your Security Management appliance, as described in [Preparing For and Managing URL Category Set Updates , on page 358](#).

When these updates occur, data for old categories will continue to appear in reports and web tracking results until the data is too old to be included. Report data generated after a category set update will use the new categories, so you may see both old and new categories in the same report.

If there is overlap between the contents of old and new categories, you may need to examine report results more carefully to obtain valid statistics. For example, if the “Instant Messaging” and “Web-based Chat” categories have been merged into a single “Chat and Instant Messaging” category during the time frame that you are looking at, visits before the merge to sites covered by the “Instant Messaging” and “Web-based Chat” categories are not counted in the total for “Chat and Instant Messaging”. Likewise, visits to instant messaging or Web-based chat sites after the merge would not be included in the totals for the “Instant Messaging” or “Web-based Chat” categories.

Using The URL Categories Page in Conjunction with Other Reporting Pages

The URL Categories page can be used in conjunction with the [Application Visibility Page, on page 199](#) and the [Users Page, on page 207](#) to investigate a particular user and the types of applications or websites that a particular user is trying to access.

For example, from the [URL Categories Page, on page 204](#) 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 [Users Page, on page 207](#), 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 displays the [Searching for Transactions Processed by Web Proxy Services, on page 229](#) on 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, on page 627](#).

Reporting Misclassified and Uncategorized URLs

You can report misclassified and uncategorized URLs at the following URL:

<https://talosintelligence.com/tickets>.

Submissions are evaluated for inclusion in subsequent rule updates.

To check the status of submitted URLs, click the **Status on Submitted URLs** tab on this page.

Application Visibility Report



Note For detailed information on Application Visibility, see the ‘Understanding Application Visibility and Control’ chapter in AsyncOS for Cisco Web Security Appliances 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 AsyncOS for Cisco Web Security Appliances User Guide.

From the **Application Visibility** page, you can view the following information:

Table 49: Details on the Web Reporting Application Visibility 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 Choosing a Time Range for Reports , on page 26.
Top Application Types by Total Transactions	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.
Top Applications by Blocked Transactions	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.
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 Working with Web Security Reports, on page 167.</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 Items Displayed 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 Find Application.</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).



Note You can generate a scheduled report for information on the Application Visibility page. For information on scheduling a report, see the [About Scheduled and On-Demand Web Reports, on page 220](#).

Anti-Malware Report

The **Web > Reporting > Anti-Malware** page is a security-related reporting page that reflects the results of scanning by your enabled scanning engines (Webroot, Sophos, McAfee, and/or Adaptive Scanning).

Use this page to help identify and monitor web-based malware threats.



Note To view data for malware found by L4 Traffic Monitoring, see [L4 Traffic Monitor Report , on page 189](#).

From the **Anti-Malware** page, you can view the following information:

Table 50: Details on the Web Reporting Anti-Malware 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 Choosing a Time Range for Reports , on page 26 .
Top Malware Categories: Monitored or Blocked	This section displays the top malware categories that are detected by a given category type. This information is displayed in graph format. See Malware Category Descriptions, on page 181 for more information on valid Malware categories.
Top Malware Threats: Monitored or Blocked	This section displays the top malware threats. This information is displayed in graph format.
Malware Categories	<p>The Malware Categories interactive table shows detailed information about particular malware categories that are displayed in the Top Malware Categories chart.</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>Exception: an Outbreak Heuristics link in the table lets you view a chart showing when transactions in this category occurred.</p> <p>See Malware Category Descriptions, on page 181 for more information on valid Malware categories.</p>
Malware Threats	<p>The Malware Threats interactive table shows detailed information about particular malware threats that are displayed in the Top Malware Threats section.</p> <p>Threats labeled “Outbreak” with a number are threats identified by the Adaptive Scanning feature independently of other scanning engines.</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Malware Category Report

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, choose **Web** from the dropdown list.
- Step 2** Choose **Monitoring > Anti-Malware** page.
- Step 3** In the Malware Categories interactive table, click on a category in the Malware Category column.
- Step 4** To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Malware Threat Report

The Malware Threat Report page 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 view this report, click a category in the Malware Category column of the Anti-Malware report page.

For additional information, click the **Support Portal Malware Details** link below the table.

Malware Category Descriptions

The Web Security Appliance can block the following types of malware:

Malware Type	Description
Adware	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.
Browser Helper Object	A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	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.

Malware Type	Description
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	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.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Outbreak Heuristics	This category represents malware found by Adaptive Scanning independently of the other anti-malware engines.
Phishing URL	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.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following actions: Overtly or covertly records system processes and/or user action. 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 passphrases 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.

Advanced Malware Protection (File Reputation and File Analysis) Reports

- [Requirements for File Analysis Report Details](#) , on page 183
- [Identifying Files by SHA-256 Hash](#) , on page 184

- [Advanced Malware Protection \(File Reputation and File Analysis\) Report Pages](#) , on page 185
- [Viewing File Reputation Filtering Data in Other Reports](#) , on page 186
- [About Web Tracking and Advanced Malware Protection Features](#) , on page 240

Requirements for File Analysis Report Details

- [\(Cloud File Analysis\) Ensure That the Management Appliance Can Reach the File Analysis Server](#) , on page 183
- [\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#) , on page 183
- [\(On-Premises File Analysis\) Activate the File Analysis Account](#) , on page 184
- [Additional Requirements](#) , on page 184

(Cloud File Analysis) Ensure That the Management Appliance Can Reach the File Analysis Server


In order to obtain File Analysis report details, the appliance must be able to connect to the File Analysis server over port 443. See details in [Firewall Information](#), on page 621.

If your Cisco Content Security Management appliance does not have a direct connection to the internet, configure a proxy server for this traffic (See [Upgrade and Update Settings](#), on page 488.) If you have already configured the appliance to use a proxy to obtain upgrades and service updates, the existing settings are used.

If you use an HTTPS proxy, the proxy must not decrypt the traffic; use a pass-through mechanism for communications with the File Analysis server. The proxy server must trust the certificate from the File Analysis server, but need not provide its own certificate to the File Analysis server.

(Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results

In order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization, you need to join all appliances to the same appliance group.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Select **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** Scroll to the File Analysis section.
- Step 4** If your managed appliances are pointed at different File Analysis cloud servers, select the server from which to display result details.
- Result details will not be available for files processed by any other cloud server.
- Step 5** Enter the Analysis Group ID.
- If you enter the Group ID incorrectly or need to change it for any other reason, you must open a case with Cisco TAC.
 - This change takes effect immediately; it does not require a Commit.
 - It is suggested to use your CCOID for this value.
 - This value is case-sensitive.

- This value must be identical on all appliances that will share data about files that are uploaded for analysis.
- An appliance can belong to only one group.
- You can add a machine to a group at any time, but you can do it only once.

Step 6 Click **Group Now**.

Step 7 Configure the same group on each Web Security appliance that will share data with this appliance.

What to do next

Related Topics

[For Which Files Are Detailed File Analysis Results Visible in the Cloud? , on page 186](#)

(On-Premises File Analysis) Activate the File Analysis Account

If you have deployed an on-premises (private cloud) Cisco AMP Threat Grid Appliance, you must activate the File Analysis account for your Cisco Content Security Management appliance in order to view report details available on the Threat Grid appliance. You generally only need to do this once.

Before you begin

Ensure that you are receiving System alerts at Critical level.

Step 1 The first time you attempt to access File Analysis report details from the Threat Grid appliance, wait a few minutes and you will receive an alert that includes a link.

If you do not receive this alert, click on the  icon to load the legacy web interface and choose **Management Appliance > System Administration > Alerts** and click **View Top Alerts**.

Step 2 Click the link in the alert message.

Step 3 If necessary, sign in to your Cisco AMP Threat Grid Appliance.

Step 4 Activate your management appliance account.

Additional Requirements

For any additional requirements, see the Release Notes for your Security Management appliance release, available from <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format). To identify the filenames associated with a malware instance in your organization, select Advanced Malware Protection report page and click an SHA-256 link in the table. The details page shows associated filenames.

Advanced Malware Protection (File Reputation and File Analysis) Report Pages

Report	Description
Advanced Malware Protection	<p>Shows file-based threats that were identified by the file reputation service.</p> <p>To see the users who tried to access each SHA, and the filenames associated with that SHA-256, click a SHA-256 in the table.</p> <p>Clicking the link at the bottom of Malware Threat File Details report page displays all instances of the file in Web Tracking that were encountered within the maximum available time range, regardless of the time range selected for the report.</p> <p>For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.</p> <p>If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.</p> <p>The Malware Files by Category section shows the percentage of blocked listed file SHAs received from the AMP for Endpoints console that are categorised as Custom Detection</p> <p>The threat name of a blocked listed file SHA obtained from AMP for Endpoints console is displayed as Simple Custom Detection in the Malware Threat Files section of the report.</p> <p>To view the file trajectory details of a blocked listed file SHA in the AMP for Endpoints console, perform the following steps:</p> <ol style="list-style-type: none"> 1. Choose Reporting > Advanced Malware Protection. 2. Click on the file SHA link for which you want to view the trajectory details. 3. Click on the AMP Console link in the More Details section.
File Analysis	<p>Displays the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.</p> <p>To view more than 1000 File Analysis results, export the data as a .csv file.</p> <p>For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are included in the allowed list on the Cisco AMP Threat Grid appliance show as "clean." For information about allowed list, see the AMP Threat Grid online help.</p> <p>Drill down to view detailed analysis results, including the threat characteristics and score for each file.</p> <p>You can also view additional details about an SHA directly on the server that performed the analysis by searching for the SHA or by clicking the Cisco AMP Threat Grid link at the bottom of the file analysis details page.</p> <p>To view details on the server that analyzed a file, see Requirements for File Analysis Report Details, on page 183.</p> <p>If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.</p>

Report	Description
AMP Verdict Updates	<p>Lists the files processed by this appliance for which the verdict has changed since the transaction was processed. For more information about this situation, see the documentation for your Web Security appliance.</p> <p>To view more than 1000 verdict updates, export the data as a .csv file.</p> <p>In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.</p> <p>If multiple Web Security appliances have different verdict updates for the same file, the result with the latest time stamp is displayed.</p> <p>Clicking an SHA-256 link displays web tracking results for all transactions that included this SHA-256 within the maximum available time range, regardless of the time range selected for the report.</p> <p>To view all affected transactions for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report), click the link at the bottom of the Malware Threat Files page.</p>

Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A "Blocked by Advanced Malware Protection" column may be hidden by default in applicable reports. To display additional columns, click the Columns link below the table.

For Which Files Are Detailed File Analysis Results Visible in the Cloud?

If you have deployed public-cloud File Analysis, you can view detailed results for all files uploaded from any managed appliance that has been added to the appliance group for File Analysis.

If you have added your management appliance to the group, you can view the list of managed appliances in the group by clicking the button on the **Management Appliance > Centralized Services > Security Appliances** page.

Appliances in the analysis group are identified by the File Analysis Client ID. To determine this identifier for a particular appliance, look in the following location:

Appliance	Location of File Analysis Client ID
Email Security appliance	Advanced Settings for File Analysis section on the Security Services > File Reputation and Analysis page.
Web Security appliance	Advanced Settings for File Analysis section on the Security Services > Anti-Malware and Reputation page.
Cisco Content Security Management appliance	At the bottom of the Management Appliance > Centralized Services > Security Appliances page.

Related Topics

[\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#) , on page 183

Client Malware Risk Report

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, the Client Malware Risk page lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM). A computer that connects frequently to malware sites may be infected with malware that is trying to connect to a central command and control server and should be disinfected.

The following table describes the information on the Client Malware Risk page.

Table 51: Client Malware Risk Report Page Components

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report. For more information, see Choosing a Time Range for Reports , on page 26.
Web Proxy: Top Clients Monitored or Blocked	This chart displays the top ten users that have encountered a malware risk.
L4 Traffic Monitor: Malware Connections Detected	This chart displays the IP addresses of the ten computers in your organization that most frequently connect to malware sites. This chart is the same as the “Top Client IPs” chart on the L4 Traffic Monitor Report , on page 189. See that section for more information and chart options.
Web Proxy: Client Malware Risk	The Web Proxy: Client Malware Risk table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section. You can click each user in this table to view the User Details page associated with that client. For information about that page, see the User Details (Web Reporting) , on page 173. Clicking on any of the links in the 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 ID / Client IP Address” column takes you to a User page for that user.
L4 Traffic Monitor: Clients by Malware Risk	This table displays IP addresses of computers in your organization that frequently connect to malware sites. This table is the same as the “Client Source IPs” table on the L4 Traffic Monitor Report , on page 189. For information about working with this table, see that section.



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Web Reputation Filters Report

The **Web > Reporting > Web Reputation Filters** 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 assign 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 statistical 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 the IronPort AsyncOS for Web User Guide.

From the **Web Reputation Filters** page, you can view the following information:

Table 52: Details on the Web Reporting Web Reputation Filters 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 Choosing a Time Range for Reports , on page 26.

Section	Description
Web Reputation Actions (Trend)	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.
Web Reputation Actions (Volume)	This section displays the web reputation action volume in percentages by transactions.
Web Reputation Threat Types Blocked by WBRs	This section displays the types of threats found in transactions that were blocked by Web Reputation filtering. Note: WBRs cannot always identify the threat type.
Threat Types Detected in Other Transactions	This section displays the type of threats found in transactions that were not blocked by Web Reputation filtering. Reasons these threats might not have been blocked include: <ul style="list-style-type: none"> • Not all threats have a score that meets the threshold for blocking. However, other features of the appliance may catch these threats. • Policies might be configured to allow threats to pass through. Note: WBRs cannot always identify the threat type.
Web Reputation Actions (Breakdown by Score)	If Adaptive Scanning is not enabled, this interactive table displays the Web Reputation scores broken down for each action.



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Adjusting Web Reputation Settings

Based on your report results, you may want to adjust the configured web reputation settings, for example adjust the threshold scores or enable or disable Adaptive Scanning. For specific information about configuring web reputation settings, see *AsyncOS for Cisco Web Security Appliances User Guide*.

L4 Traffic Monitor Report

The **Web > Reporting > L4 Traffic Monitor** page displays information about malware ports and malware sites that the L4 Traffic Monitors on your Web Security appliances have detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

The L4 Traffic Monitor listens to network traffic that comes in over all ports on each Web Security appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

You can use data in this report to determine whether to block a port or a site, or to investigate why a particular client IP address is connecting unusually frequently to a malware site (for example, this could be because the computer associated with that IP address is infected with malware that is trying to connect to a central command and control server.)



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Table 53: L4 Traffic Monitor Report Page Components

Section	Description
Time Range (drop-down list)	A menu that allows you to choose a time range on which to report. For more information, see Choosing a Time Range for Reports, on page 26 .
Top Client IPs	<p>This section displays, in graph format, the IP addresses of computers in your organization that most frequently connect to malware sites.</p> <p>Click the Chart Options link below the chart to change the display from total Malware Connections Detected to Malware Connections Monitored or Malware Connections Blocked.</p> <p>This chart is the same as the “L4 Traffic Monitor: Malware Connections Detected” chart on the Client Malware Risk Report, on page 187.</p>
Top Malware Sites	<p>This section displays, in graph format, the top malware domains detected by the L4 Traffic Monitor.</p> <p>Click the Chart Options link below the chart to change the display from total Malware Connections Detected to Malware Connections Monitored or Malware Connections Blocked.</p>
Client Source IPs	<p>This table displays the IP addresses of computers in your organization that frequently connect to malware sites.</p> <p>To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Port. You can use this feature to help determine which ports are used by malware that “calls home” to malware sites.</p> <p>To view details such as the port and destination domain of each connection, click an entry in the table. For example, if one particular client IP address has a high number of Malware Connections Blocked, click the number in that column to view a list of each blocked connection. The list is displayed as search results in the L4 Traffic Monitor tab on the Web > Reporting > Web Tracking page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor, on page 233.</p> <p>This table is the same as the “L4 Traffic Monitor - Clients by Malware Risk” table on the Client Malware Risk Report, on page 187.</p>
Malware Ports	<p>This table displays the ports on which the L4 Traffic Monitor has most frequently detected malware.</p> <p>To view details, click an entry in the table. For example, click the number of Total Malware Connections Detected to view details of each connection on that port. The list is displayed as search results in the L4 Traffic Monitor tab on the Web > Reporting > Web Tracking page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor, on page 233.</p>

Section	Description
Malware Sites Detected	<p>This table displays the domains on which the L4 Traffic Monitor most frequently detects malware.</p> <p>To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Port. You can use this feature to help determine whether to block a site or a port.</p> <p>To view details, click an entry in the table. For example, click the number of Malware Connections Blocked to view the list of each blocked connection for a particular site. The list is displayed as search results in the L4 Traffic Monitor tab on the Web > Reporting > Web Tracking page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 233.</p>



Tip To customize your view of this report, see [Working with Web Security Reports](#), on page 167.

Related Topics

- [Troubleshooting L4 Traffic Monitor Reports](#) , on page 243

SOCKS Proxy Report

The **Web > Reporting > SOCKS Proxy** Page allows you to view data and trends for transactions processed through the SOCKS proxy, including information about destinations and users.



Note The destination shown in the report is the address that the SOCKS client (typically a browser) sends to the SOCKS proxy.

To change SOCKS policy settings, see AsyncOS for Cisco Web Security Appliances User Guide.

Related Topics

- [Searching for Transactions Processed by the SOCKS Proxy](#) , on page 234

Reports by User Location

The **Web > Reporting > Reports by User Location** Page allows you to find out what activities 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.

From the **Reports by User Location** page, you can view the following information:

Table 54: 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 Choosing a Time Range for Reports , on page 26.
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.



Tip To customize your view of this report, see [Working with Web Security Reports](#), on page 167.



Note You can generate a scheduled report for information on the Reports by User Location page. For information on scheduling a report, see the [About Scheduled and On-Demand Web Reports](#), on page 220.

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.

Viewing the System Capacity Report

Step 1 On the Security Management appliance, choose **Web > Reporting > System Capacity**.

Step 2 To view different types of data, click **Columns** and choose the data to view.

Step 3 To see the system capacity for a single appliance, click the appliance in the Web Security appliance column in the Overview of Averaged Usage and Performance table.

The System Capacity graphs appear for that appliance. The graphs on the page are divided into two sets:

- [System Capacity - System Load](#) , on page 193
- [System Capacity - Network Load](#) , on page 194

How to Interpret the Data You See on the 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 for other reports, we recommend that you select the largest time range, 90 days.

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.

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.

The Proxy Buffer Memory may indicate spikes in network traffic during normal operation, but if the graph climbs steadily to the maximum, the appliance may be reaching its maximum capacity and you should consider adding capacity.

These charts are on the same page as the charts described in [System Capacity - System Load](#), on page 193, below those charts.

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 Web Security appliances to your network or tune your configuration to ensure maximum throughput to improve performance.

Data Availability Page

The **Web > Reporting > Data Availability** page provides an overview of the date ranges for which reporting and web tracking data are available on the Security Management appliance for each managed Web Security appliance.



Note 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.

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.

For information about purging of data, see the [Managing Disk Space](#), on page 521.



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.

Understanding the Web Reporting Pages on the New Web Interface

The following table lists the reports under the Reports drop-down, available in the latest supported release of AsyncOS for Web Security appliances under the **Reports** drop-down of the web interface. For more information, see [Using the Interactive Report Pages, on page 37](#). If your Web Security appliances are running earlier releases of AsyncOS, not all of these reports are available.

Table 55: Web Reports Drop-down Options

Reports Drop-down Option	Action
General Reports	
Overview Page	The Overview page provides a synopsis of the activity on your Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the Overview Page, on page 197 .
Application Visibility Page	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 Application Visibility Page, on page 199 .
Layer 4 Traffic Monitor Page	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 Layer 4 Traffic Monitor Page, on page 201 .
SOCKS Proxy Page	Allows you to view data for SOCKS proxy transactions, including destinations and users. For more information, see the SOCKS Proxy Page, on page 203 .

Reports Drop-down Option	Action
URL Categories Page	<p>The URL Categories page allows you to view the top URL Categories that are being visited, including:</p> <ul style="list-style-type: none"> • The top URLs that have triggered a block or warning action to occur per transaction. • 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. <p>For more information, see the URL Categories Page, on page 204.</p>
Users Page	<p>The Users page provides several web tracking links that allow you to view web tracking information for individual users.</p> <p>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.</p> <p>From the Users 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 User Details page allows you to see specific information about a user that you have identified in the Users table on the Users 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 Users Page, on page 207.</p> <p>For information on a specific user in your system, see the User Details Page (Web Reporting), on page 208.</p>
Web Sites Page	<p>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 Web Sites Page, on page 210.</p>
HTTPS Reports	<p>The HTTPS Reports report page is an overall aggregation of the HTTP/HTTPS traffic summary (transactions or bandwidth usage) on the managed appliances. For more information, see the HTTPS Reports Page, on page 211.</p>
Threat Reports	

Reports Drop-down Option	Action
Anti-Malware Page	The Anti-Malware page allows you to view information about malware ports and malware sites that the anti-malware scanning engine(s) 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 Anti-Malware Page , on page 212.
Client Malware Risk Page	The Client Malware Risk page is a security-related reporting page that can be used to identify individual client computers that may be connecting unusually frequently to malware sites. For more information, see the Client Malware Risk Report , on page 217.
Web Reputation Filters Page	Allows you to view reporting on Web Reputation filtering for transactions during a specified time range. For more information, see the Web Reputation Filters Page , on page 218.

About Time Spent

The Time Spent column in various tables represents the amount of time a user 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.

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.

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.

For the purposes of the time spent value, considering the following notes:

- An active user is defined as a user name or IP address that sends HTTP traffic through the appliance and has gone to a website that AsyncOS considers to be a “page view.”
- 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.

Units are displayed in Hours:Minutes format.

Overview Page

The **Overview** report page provides a synopsis of the activity on your Web Security appliances. It includes graphs and summary tables for the incoming and outgoing transactions.

To view the Overview report page, select **Web** from the Product drop-down and choose **Monitoring > Overview** from the Reports drop-down. For more information, see [Using the Interactive Report Pages](#), on page 37.

At a high level the **Overview** report 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 report 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.

Table 56: Details on the Overview Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
View Data for (drop-down list)	Choose a Web Security appliance for which you want to view Overview data, or choose All Web Appliances. See also Viewing Reporting Data for an Appliance or Reporting Group , on page 25
Total Web Proxy Activity	You can view the web proxy activity that is being reported by the Web Security appliances that are currently managed by the Security Management appliance. This section displays the actual number of transactions and the approximate date that the activity occurred in graphical format. You can also view the percentage of web proxy activity that are suspect, or clean proxy activity, including the total number of transactions.
Suspect Transactions	You can view the web transactions that have been labeled as suspect by the administrator in a graphical format. This section displays the actual number of transactions and the approximate date that the activity occurred, in graphical format. You can also 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.
L4 Traffic Monitor Summary	You can view any L4 traffic that is being reported by the Web Security appliances that are currently managed by the Security Management appliance, in graphical format.
Top URL Categories: Total Transactions	You can view the top URL categories that are being blocked, including the type of URL category and the actual number of times the specific type of category has been blocked in graphical format. The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 177.

Section	Description
Top Application Types: Total Transactions	You can view the top application types that are being blocked, including the name of the actual application type and the number of times the specific application has been blocked, in graphical format.
Top Malware Categories: Monitored or Blocked	You can view all the Malware categories that have been detected, in graphical format.
Top Users: Blocked or Warned Transactions	You can view the actual users that are generating the blocked or warned transactions, in graphical format. Users can be displayed by IP address or by user name. To make user names unrecognizable, see Anonymizing User Names in Web Reports , on page 166.

Application Visibility Page



Note For detailed information on Application Visibility, see the ‘Understanding Application Visibility and Control’ chapter in User Guide for AsyncOS for Cisco Web Security Appliances.

The **Application Visibility** report page allows you to apply controls to particular application types within the Security Management appliance and Web Security appliance.

To view the Application Visibility report page, select **Web** from the product drop-down and choose **Monitoring > Application Visibility** from the Reports drop-down. For more information, see [Using the Interactive Report Pages](#), on page 37.

The application control gives you more granular control over web traffic than just URL filtering, for example, as well as 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 User Guide for AsyncOS for Cisco Web Security Appliances.

From the Application Visibility page, you can view the following information:

Table 57: Details on the Application Visibility Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Top Application Types by Total Transactions	<p>You can view the top application types that are being visited on the site in graphical format.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p> <p>For example, instant messaging tools such as Yahoo Instant Messenger, Facebook, and Presentation application types.</p>
Top Applications by Blocked Transactions	<p>You can view the top application types that triggered a block action to occur per transaction in graphical format.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p> <p>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.</p>
Application Types Matched	<p>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.</p> <p>From the Applications column you can click on an application to view details.</p>
Applications Matched	<p>The Applications Matched interactive table shows all the application during a specified time range.</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 Find Application.</p>



Note To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Layer 4 Traffic Monitor Page



The **Layer 4 Traffic Monitor** report page displays information about malware ports and malware sites that the Layer 4 Traffic Monitors on your Web Security appliances have detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

To view the Web Sites report page, select **Web** from the Product drop-down and choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The Layer 4 Traffic Monitor listens to network traffic that comes in over all ports on each Web Security appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

You can use data in this report to determine whether to block a port or a site, or to investigate why a particular client IP address is connecting unusually frequently to a malware site (for example, this could be because the computer associated with that IP address is infected with malware that is trying to connect to a central command and control server.)

Table 58: Details on the Layer 4 Traffic Monitor Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Top Client IPs: Malware Connections Detected	<p>You can view the top IP addresses of computers in your organization that most frequently connect to malware sites, in graphical format.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p> <p>This chart is the same as the “Layer 4 Traffic Monitor: Malware Connections Detected” chart on the Client Malware Risk Report, on page 217.</p>
Top Malware Sites: Malware Connections Detected	<p>You can view the top malware domains detected by the Layer 4 Traffic Monitor, in graphical format.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>

Section	Description
Client Source IPs	<p>You can use the this interactive table to view the IP addresses of computers in your organization that frequently connect to malware sites.</p> <p>To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Client IP. You can use this feature to help determine which ports are used by malware that “calls home” to malware sites.</p> <p>To view details such as the port and destination domain of each connection, click an entry in the table. For example, if one particular client IP address has a high number of Malware Connections Blocked, click the number in that column to view a list of each blocked connection. The list is displayed as search results in the Layer 4 Traffic Monitor tab of the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 233.</p> <p>This chart is the same as the “Layer 4 Traffic Monitor: Malware Connections Detected” chart on the Client Malware Risk Report , on page 217.</p>
Malware Ports	<p>You can use the this interactive table to view the ports on which the Layer 4 Traffic Monitor has most frequently detected malware.</p> <p>To view details, click an entry in the table. For example, click the number of Total Malware Connections Detected to view details of each connection on that port. The list is displayed as search results in the Layer 4 Traffic Monitor tab on the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 233.</p>
Malware Sites Detected	<p>You can use the this interactive table to view the domains on which the Layer 4 Traffic Monitor most frequently detects malware.</p> <p>To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Port. You can use this feature to help determine whether to block a site or a port.</p> <p>To view details, click an entry in the table. For example, click the number of Malware Connections Blocked to view the list of each blocked connection for a particular site. The list is displayed as search results in the Layer 4 Traffic Monitor tab on the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the L4 Traffic Monitor , on page 233.</p>



Tip To customize your view of this report, see [Working with Web Security Reports](#), on page 167.

Related Topics

[Troubleshooting L4 Traffic Monitor Reports](#) , on page 243

SOCKS Proxy Page

The SOCKS Proxy report page allows you to view transactions processed through the SOCKS proxy, including information about destinations and users, in a graphical and tabular format.

To view the SOCKS Proxy report page, select **Web** from the product drop-down and choose **Monitoring > SOCKS Proxy** from the Reports drop-down. For more information, see [Using the Interactive Report Pages](#), on page 37.



Note The destination shown in the report is the address that the SOCKS client (typically a browser) sends to the SOCKS proxy.

To change SOCKS policy settings, see *User Guide for AsyncOS for Cisco Web Security Appliances*.

Table 59: Details on the SOCKS Proxy Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Top Destinations for SOCKS: Total Transactions	You can view the top destinations detected by the SOCKS proxy, in graphical format. To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart , on page 39.
Top Users for SOCKS: Malware Transactions	You can view the top users detected by the SOCKS proxy, in graphical format. To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart , on page 39.
Destinations	You can use the this interactive table to view the list of destination domains or IP addresses processed through SOCKS proxy. To include only data for a particular destination, enter a domain name or IP address into the box at the bottom of the table and click Find Domain or IP .

Section	Description
Users	<p>You can use the this interactive table to view the list of users or IP addresses processed through SOCKS proxy.</p> <p>To include only data for a particular user, enter a user name or IP address into the box at the bottom of the table and click Find User ID / Client IP Address.</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Related Topics

[Searching for Transactions Processed by the SOCKS Proxy , on page 234](#)

URL Categories Page



The **URL Categories** report page can be used to view the URL categories of sites that users on your system are visiting.

To view the URL Categories report page, select **Web** from the Product drop-down and choose **Monitoring > URL Categories** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the URL Categories page, you can view the following information:

Table 60: Details on the URL Categories Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26 .
Top URL Categories: Total Transactions	<p>You can view the top URL Categories that are being visited on the site in a graphical format.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>
Top URL Categories: Blocked and Warned Transactions	<p>You can view the top URL that triggered a block or warning action to occur per transaction in a graphical 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.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>

Section	Description
Top Youtube Categories: Total Transactions	<p>You can view the top Youtube Categories that are being visited on the site in a graphical format.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart , on page 26.</p>
Top Youtube Categories: Blocked and Warned Transactions	<p>You can view the top Youtube URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain Youtube URL and because of a specific policy that is in place, this triggered a block action or a warning. This Youtube URL then gets listed in this graph as a transaction blocked or warning.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart , on page 26 .</p>
URL Categories Matched	<p>The URL Categories Matched interactive table shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category.</p> <p>If there are a large number of unclassified URLs, see Reducing Uncategorized URLs , on page 177.</p>
Youtube Categories Matched	<p>The Youtube Categories Matched interactive table shows the disposition of transactions by Youtube category during the specified time range, plus bandwidth used and time spent in each category.</p> <p>To view the Youtube Categories Matched interactive table, choose Web > Reporting > URL Categories .</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Reducing Uncategorized URLs

If the percentage of uncategorized URLs is higher than 15-20%, consider the following options:

- For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. These transactions will then be included in “URL Filtering Bypassed” statistics instead. To do this, see information about custom URL categories AsyncOS for Cisco Web Security Appliance s User Guide.
- For sites that you feel should be included in existing or other categories, see [Reporting Misclassified and Uncategorized URLs](#) , on page 178.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated on your Security Management appliance, as described in [Preparing For and Managing URL Category Set Updates](#), on page 358.

When these updates occur, data for old categories will continue to appear in reports and web tracking results until the data is too old to be included. Report data generated after a category set update will use the new categories, so you may see both old and new categories in the same report.

If there is overlap between the contents of old and new categories, you may need to examine report results more carefully to obtain valid statistics. For example, if the “Instant Messaging” and “Web-based Chat” categories have been merged into a single “Chat and Instant Messaging” category during the time frame that you are looking at, visits before the merge to sites covered by the “Instant Messaging” and “Web-based Chat” categories are not counted in the total for “Chat and Instant Messaging”. Likewise, visits to instant messaging or Web-based chat sites after the merge would not be included in the totals for the “Instant Messaging” or “Web-based Chat” categories.

Using The URL Categories Page in Conjunction with Other Reporting Pages

The URL Categories page can be used in conjunction with the [Application Visibility Page](#), on page 199 and the [Users Page](#), on page 207 to investigate a particular user and the types of applications or websites that a particular user is trying to access.

For example, from the [URL Categories Page](#), on page 204 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 [Users Page](#), on page 207, 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 displays the [Searching for Transactions Processed by Web Proxy Services](#), on page 229 on 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](#), on page 627.

Reporting Misclassified and Uncategorized URLs

You can report misclassified and uncategorized URLs at the following URL:

<https://talosintelligence.com/tickets>.

Submissions are evaluated for inclusion in subsequent rule updates.

To check the status of submitted URLs, click the **Status on Submitted URLs** tab on this page.

Users Page

The **Users** report page provides several links that allow you to view web reporting information for individual users.

To view the Users report page, select **Web** from the Product drop-down and choose **Monitoring > Users** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

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.

From the **Users** page, you can view the following information pertaining to the users on your system:

Table 61: Details on the Users Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Top Users: Transactions Blocked	<p>You can view the top users, by either IP address or user name, and the number of transactions that have been blocked specific to that user, in graphical format. 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 Enabling Centralized Web Reporting on the Security Management Appliance , on page 165. The default setting is that all user names appear. To hide user names, see Anonymizing User Names in Web Reports , on page 166.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>
Top Users: Bandwidth Used	<p>You can view the top users, by either IP address or user name, that are using the most bandwidth on the system, in graphical format.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>

Section	Description
Users	<p>You can use this interactive table to search for a specific User ID or Client IP address. In the text field at the bottom of the User table, enter the specific User ID or Client IP address and click on Find User ID / Client IP Address. The IP address does not need to be an exact match to return results.</p> <p>You can click on a specific user to find more specific information. For more information, see the User Details Page (Web Reporting), on page 208</p>



Note To view user IDs instead of client IP addresses, you must set up your Security Management appliance to obtain user information from an LDAP server.



Tip To customize your view of this report, see [Working with Web Security Reports](#), on page 167.

User Details Page (Web Reporting)

The **User Details** page allows you to see specific information about a user that you have identified in the interactive table on the Users report 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 Users interactive table on the **Users** report page.

From the User Details page, you can view the following information pertaining to an individual user on your system:

Table 62: Details on the User Details Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
URL Categories: Total Transactions	<p>You can view the specific URL Categories that a specific user is using, in graphical format.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart.</p> <p>The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports, on page 177.</p>

Section	Description
Trend: Total Transactions	<p>You can use this trend graph to view all the web transactions of a specific user.</p> <p>To customize the view of the chart, click  on the chart.</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>
URL Categories Matched	<p>The URL Categories Matched interactive table shows matched categories for both completed and blocked transactions.</p> <p>You can search for a specific URL Category in the text field at the bottom of the table and click Find URL Category. The category does not need to be an exact match.</p> <p>The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 177.</p>
Domains Matched	<p>The Domains Matched interactive table shows domains or IP addresses that the user has accessed. You can also view the time spent on those categories, and various other information that you have set from the column view.</p> <p>You can search for a specific Domain or IP address in the text field at the bottom of the table and click Find Domain or IP. The domain or IP address does not need to be an exact match.</p>
Applications Matched	<p>The Applications Matched interactive table shows applications 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>You can search for a specific application name in the text field at the bottom of the table and click Find Application. The name of the application does not need to be an exact match.</p>
Advanced Malware Protection Threats Detected	<p>The Advanced Malware Protection Threats Detected interactive table shows malware threat files that are detected by the Advanced Malware Protection engine.</p> <p>You can search for data on a specific SHA value of the malware threat file, in the text field at the bottom of the table and click Find malware Threat File SHA 256. The name of the application does not need to be an exact match.</p>

Section	Description
Malware Threats Detected	The Malware Threats Detected interactive table shows the top Malware threats that a specific user is triggering. You can search for data on a specific malware threat name in the text field at the bottom of the table and click Find Malware Threat . The name of the Malware Threat does not need to be an exact match.
Policies Matched	The Policies Matched interactive table shows the policy groups that applied to this user when accessing the web. You can search for a specific policy name in the text field at the bottom of the table and click Find Policy . The name of the policy does not need to be an exact match.



Note From Client Malware Risk Details table: 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 Sites Page


The **Web Sites** report page is an overall aggregation of the activity that is happening on the managed appliances. You can use this report page to monitor high-risk web sites accessed during a specific time range.

To view the Web Sites report page, select **Web** from the Product drop-down and choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

From the Web Sites page, you can view the following information:

Table 63: Details on the Web Sites Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Top Domains: Total Transactions	You can view the top domains that are being visited on the website in graphical format. To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39 .

Section	Description
Top Domains: Transactions Blocked	<p>You can view the top domains that triggered a block action to occur per transaction in graphical format.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p> <p>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 is listed in this graph as a transaction blocked, and the domain site that triggered the block action is listed.</p>
Domains Matched	<p>You can use this interactive table to search for the domains that are that are being visited on the website. You can click on a specific domain to access more granular information. The Proxy Services tab on the Web Tracking page appears and you can see tracking information and why certain domains were blocked.</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.</p> <p>To view an example of how Web Tracking may be used, see Example 2: Tracking a URL, on page 627.</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

HTTPS Reports Page

The HTTPS Reports report page is an overall aggregation of the HTTP/HTTPS traffic summary (transactions or bandwidth usage) on the managed appliances.

You can also view the summary of supported ciphers based on either client side connections or server side connections, for individual HTTP/HTTPS web traffic that passes through the managed appliance.

To view the HTTPS Reports report page, select **Web** from the **Product** drop-down and choose **Monitoring > HTTPS Reports** from the **Reports** drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

Table 64: Details on the HTTPS Reports Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.

Section	Description
Web Traffic Summary	<p>You can view the web traffic summary on the appliance in one of the following ways:</p> <ul style="list-style-type: none"> • Transactions: Select this option from the drop-down list to display the web traffic summary based on the number of HTTP or HTTPS web transactions, in a graphical format and percentage of HTTP or HTTPS web transaction in tabular format. • Bandwidth Usage: Select this option from the drop-down list to display the web traffic summary based on the amount of bandwidth consumed by the HTTP or HTTPS web traffic, in a graphical format and the percentage of HTTP or HTTPS bandwidth usage in tabular format.
Trend: Web Traffic	<p>You can view the trend graph for the web traffic on the appliance based on the required time range in one of the following ways:</p> <ul style="list-style-type: none"> • Web Traffic Trend: Select this option from the dropdown list to display the cumulative trend for HTTP and HTTPS web traffic based on the transactions or bandwidth usage. • HTTPS Trend: Select this option from the dropdown list to display the trend for HTTPS web traffic based on the transactions or bandwidth usage. • HTTP Trend: Select this option from the dropdown list to display the trend for HTTP web traffic based on the transactions or bandwidth usage.
Ciphers	<p>You can view the summary of the ciphers in one of the following ways:</p> <ul style="list-style-type: none"> • By Client Side Connections: Select this option from the dropdown list to display the summary of the ciphers used on the client side of the HTTP or HTTPS web traffic in a graphical format. • By Server Side Connections: Select this option from the dropdown list to display the summary of the ciphers used on the server side of the HTTP or HTTPS web traffic in a graphical format.

Anti-Malware Page

The **Anti-Malware** report page is a security-related reporting page that reflects the results of scanning by your enabled scanning engines (Webroot, Sophos, McAfee, and/or Adaptive Scanning).

To view the Anti-Malware report page, select **Web** from the Product drop-down and choose **Monitoring > Anti-Malware** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

You can use this page to help identify and monitor web-based malware threats.



Note To view data for malware found by L4 Traffic Monitoring, see [Layer 4 Traffic Monitor Page, on page 201](#)

From the Anti-Malware page, you can view the following information:

Table 65: Details on the Anti-Malware Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Top Malware Categories	<p>You can view the top malware categories that are detected by a given category type, in graphical format. See Malware Category Descriptions, on page 181 for more information on valid Malware categories.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>
Top Malware Threats	<p>You can view the the top malware threats in graphical format.</p> <p>To customize the view of the chart, click <input checked="" type="checkbox"/> on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>
Malware Categories	<p>The Malware Categories interactive table shows detailed information about particular malware categories that are displayed in the Top Malware Categories chart.</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>Exception: an Outbreak Heuristics link in the table lets you view a chart showing when transactions in this category occurred.</p> <p>See Malware Category Descriptions, on page 181 for more information on valid Malware categories.</p>
Malware Threats	<p>The Malware Threats interactive table shows detailed information about particular malware threats that are displayed in the Top Malware Threats section.</p> <p>Threats labeled “Outbreak” with a number are threats identified by the Adaptive Scanning feature independently of other scanning engines.</p>



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Malware Category Report

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, choose **Web** from the dropdown list.
 - Step 2** Choose **Monitoring > Anti-Malware** page.
 - Step 3** In the Malware Categories interactive table, click on a category in the Malware Category column.
 - Step 4** To customize your view of this report, see [Working with Web Security Reports, on page 167](#).
-

Malware Threat Report

The Malware Threat Report page 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 view this report, click a category in the Malware Category column of the Anti-Malware report page.

For additional information, click the **Support Portal Malware Details** link below the table.

Malware Category Descriptions

The Web Security Appliance can block the following types of malware:

Malware Type	Description
Adware	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.
Browser Helper Object	A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	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.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.

Malware Type	Description
Hijacker	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.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Outbreak Heuristics	This category represents malware found by Adaptive Scanning independently of the other anti-malware engines.
Phishing URL	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.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following actions: Overtly or covertly records system processes and/or user action. 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 passphrases 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.

Advanced Malware Protection Page

Advanced Malware Protection protects against zero-day and targeted file-based threats by:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.

- Evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

For more information on the file reputation filtering and file analysis, see the user guide or online help for *AsyncOS for Web Security Appliances*.

To view the Advanced Malware Protection report page, select **Web** from the Product drop-down and choose **Monitoring > Advanced Malware Protection** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

The Advanced Malware Protection report page shows the following reporting views:

- [Advanced Malware Protection - AMP Summary, on page 216](#)
- [Advanced Malware Protection - File Analysis, on page 217](#)

Related Topics

- [Requirements for File Analysis Report Details , on page 183](#)
- [Identifying Files by SHA-256 Hash , on page 184](#)
- [Viewing File Reputation Filtering Data in Other Reports , on page 186](#)
- [About Web Tracking and Advanced Malware Protection Features , on page 240](#)

Advanced Malware Protection - AMP Summary

The AMP Summary section of the Advanced Malware Protection report page shows file-based threats that were identified by the file reputation service.

To see the users who tried to access each SHA, and the filenames associated with that SHA-256, click a SHA-256 in the table.

You can click on the link in the Malware Threat Files interactive table to view all the instances of the file in Web Tracking that were encountered within the maximum available time range, regardless of the time range selected for the report.

If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.

You can use the AMP Summary section of the Advanced Malware Protection page to view:

- The summary of files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- The top malware threat files in a graphical format.
- The top threat files based on the file types in a graphical format.
- A trend graph for all the malware threat files based on the selected time range.
- The Malware Threat Files interactive table that lists the top malware threat files.
- The Files With Retrospective Verdict Change interactive table that lists the files processed by this appliance for which the verdict has changed since the transaction was processed. For more information about this situation, see the documentation for your Web Security appliance.

In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.

If multiple Web Security appliances have different verdict updates for the same file, the result with the latest time stamp is displayed.

You can click on a SHA-256 link to view web tracking results for all transactions that included this SHA-256 within the maximum available time range, regardless of the time range selected for the report.

Advanced Malware Protection - File Analysis

The File Analysis section of the Advanced Malware Protection report page shows the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.

For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are included in the allowed list on the Cisco AMP Threat Grid appliance show as "clean." For information about allowed list, see the AMP Threat Grid online help.

Drill down to view detailed analysis results, including the threat characteristics and score for each file.

You can also view additional details about an SHA directly on the server that performed the analysis by searching for the SHA or by clicking the Cisco AMP Threat Grid link at the bottom of the file analysis details page.

To view details on the server that analyzed a file, see [Requirements for File Analysis Report Details](#), on page 183.

If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.

You can use the File Analysis section of the Advanced Malware Protection report page to view:

- The number of files that are uploaded for file analysis by file analysis service of the Advanced Malware Protection engine.
- A list of files that have completed file analysis requests.
- A list of files that have pending file analysis requests.

Client Malware Risk Report

The **Client Malware Risk** report page is a security-related reporting page that can be used to monitor client malware risk activity.



To view the Client Malware Risk report page, select **Web** from the Product drop-down and choose **Monitoring > Client Malware Risk** from the Reports drop-down. For more information, see [Using the Interactive Report Pages](#), on page 37.

From the Client Malware Risk report 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, the Client Malware Risk page lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM). A computer that connects frequently to malware sites may be infected with malware that is trying to connect to a central command and control server and should be disinfected.

The following table describes the information on the Client Malware Risk page.

Table 66: Details on Client Malware Risk Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.
Web Proxy: Top Clients Monitored or Blocked	<p>You can view the top ten users that have encountered a malware risk, in graphical format.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p>
L4 Traffic Monitor: Malware Connections Detected	<p>You can view the IP addresses of the ten computers in your organization that most frequently connect to malware sites, in graphical format.</p> <p>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39.</p> <p>This chart is the same as the “Top Client IPs” chart on the Layer 4 Traffic Monitor Page, on page 201.</p>
Web Proxy: Client Malware Risk	<p>The Web Proxy: Client 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>You can click each user in this table to view the User Details page associated with that client. For information about that page, see the User Details Page (Web Reporting) , on page 208.</p> <p>You can click on any of the links in the table to view more granular details about individual users and what activity they are performing that is triggering the malware risk.</p>
L4 Traffic Monitor: Clients by Malware Risk	<p>The L4 Traffic Monitor: Clients by Malware Risk interactive table displays IP addresses of computers in your organization that frequently connect to malware sites.</p> <p>This table is the same as the “Client Source IPs” table on the Layer 4 Traffic Monitor Page, on page 201.</p>



Tip To customize your view of this report, see [Working with Web Security Reports](#), on page 167.

Web Reputation Filters Page

You can use the **Web Reputation Filters** report page to view the results of your set Web Reputation filters for transactions during a specified time range.

To view the Web Reputation Filters report page, select **Web** from the Product drop-down and choose **Monitoring > Web Reputation Filters** from the Reports drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).

What are Web Reputation Filters?

Web Reputation Filters analyze web server behavior and assign 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 statistical 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 the *User Guide for AsyncOS for Web Security Appliances*.

From the Web Reputation Filters page, you can view the following information:

Table 67: Details on Web Reputation Filters Page

Section	Description
Time Range (drop-down list)	Choose the time range for your report. For more information, see the Choosing a Time Range for Reports , on page 26.

Section	Description
Web Reputation Actions (Trend)	You can view the total number of web reputation actions against the time specified, in graphical format. From this you can see potential trends over time for web reputation actions.
Web Reputation Actions (Volume)	You can view the web reputation action volume in percentages by transactions.
Web Reputation Threat Types Blocked by WBRs	You can view the types of threats found in transactions that were blocked by Web Reputation filtering, in graphical format. Note WBRs cannot always identify the threat type.
Threat Types Detected in Other Transactions	You can view the type of threats found in transactions that were not blocked by Web Reputation filtering, in graphical format. To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 39 . Reasons these threats might not have been blocked include: <ul style="list-style-type: none"> • Not all threats have a score that meets the threshold for blocking. However, other features of the appliance may catch these threats. • Policies might be configured to allow threats to pass through. Note WBRs cannot always identify the threat type.
Web Reputation Actions (Breakdown by Score)	If Adaptive Scanning is not enabled, this interactive table displays the Web Reputation scores broken down for each action.



Tip To customize your view of this report, see [Working with Web Security Reports, on page 167](#).

Adjusting Web Reputation Settings

Based on your report results, you may want to adjust the configured web reputation settings, for example adjust the threshold scores or enable or disable Adaptive Scanning. For specific information about configuring web reputation settings, see *User Guide for AsyncOS for Cisco Web Security Appliances*.

About Scheduled and On-Demand Web Reports

Except as noted, you can generate the following types of Web Security reports either as scheduled or on-demand reports:

- Web Reporting Overview—For information on what is included on this page, see the [Web Reporting Overview, on page 171](#).
- Users—For information on what is included on this page, see the [Users Report \(Web\), on page 172](#).

- Web Sites—For information on what is included on this page, see the [Web Sites Report](#) , on page 175.
- URL Categories—For information on what is included on this page, see the [URL Categories Report](#) , on page 176.
- Top URL Categories — Extended: For information on how to generate a report for Top URL Categories — Extended, see the [Top URL Categories—Extended](#), on page 223.

This report is not available as an On-Demand report.

- Application Visibility—For information on what is included on this page, see the [Application Visibility Report](#) , on page 178.
- Top Application Types — Extended: For information on how to generate a report for Top URL Categories — Extended, see the [Top Application Types—Extended](#), on page 224.

This report is not available as an On-Demand report.

- Anti-Malware—For information on what is included on this page, see the [Anti-Malware Report](#) , on page 180.
- Client Malware Risk—For information on what is included on this page, see the [Client Malware Risk Report](#) , on page 187.
- Web Reputation Filters—For information on what is included on this page, see the [Web Reputation Filters Report](#) , on page 188.
- L4 Traffic Monitor—For information on what is included on this page, see the [L4 Traffic Monitor Report](#) , on page 189.
- Mobile Secure Solution—For information on what is included on this page, see the [Reports by User Location](#) , on page 191.
- System Capacity—For information on what is included on this page, see the [System Capacity Page](#), on page 192.

Scheduling Web Reports

This section includes the following:

- [Adding Scheduled Web Reports](#), on page 222
- [Editing Scheduled Web Reports](#), on page 223
- [Deleting Scheduled Web Reports](#), on page 223
- [Additional Extended Web Reports](#), on page 223



Note You can choose to make user names unrecognizable in all reports. For information, see [Anonymizing User Names in Web Reports](#) , on page 166.

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 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.

My Web Report is a user report under the Scheduled Reports menu. The user reports can only be seen by the user who has created them.

Storage of Scheduled Web Reports

The Security Management appliance retains the most recent reports that it generates — up to 30 of the most recent instances of each scheduled report, and up to 1000 total versions for all reports.

Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 30 instances applies to each scheduled report with the same name and time range.

Archived reports are stored in the /periodic_reports directory on the appliance. (See [IP Interfaces and Accessing the Appliance](#), on page 609 for more information.)

Related Topics

- [Viewing and Managing Archived Web Reports](#), on page 226

Adding Scheduled Web Reports

-
- Step 1** On the Security Management appliance, choose **Web > Reporting > Scheduled Reports**.
- Step 2** Click **Add Scheduled Report**.
- 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 also allow you to save raw data as a CSV file.
- 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** For **Charts**, click the default chart under **Data to display** and choose the data to display in each chart in the report.
- Step 9** 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 10** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.
- Step 11** 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 12** Click **Submit**.
-

Editing Scheduled Web 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 Web 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 Web Reports

Two additional reports are available only as Scheduled Reports on the Security Management appliance:

- [Top URL Categories—Extended, on page 223](#)
- [Top Application Types—Extended, on page 224](#)

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. 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, use the Top URL Categories —Extended report.



Note The maximum number of reports that can be generated using this type of report is 20.

- Predefined URL category lists are occasionally updated. For more information about the impact of these updates on report results, see [URL Category Set Updates and Reports](#), on page 177.

To generate a Top URL Categories—Extended report, perform the following:

-
- Step 1** On the Security Management appliance, choose **Web > Reporting > Scheduled Reports**.
 - Step 2** Click **Add Scheduled Report**.
 - Step 3** From the 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** For **Charts**, click the default chart under **Data to display** and choose the data to display in each chart in the report.
- Step 10** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.
- Step 11** In the **Email** text field, type in the email address where the generated report will be sent.
- Step 12** Click **Submit**.

Top Application Types—Extended

To generate a Top Application Type—Extended report, perform the following:

- Step 1** On the Security Management appliance, choose **Web > Reporting > Scheduled Reports**.
- Step 2** Click **Add Scheduled Report**.
- Step 3** From the drop-down menu next to Type, choose **Top Application Types — Extended**.
The options on the page will change.
- 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 Application Types 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** For **Charts**, click a default chart under **Data to display** and choose the data to display in each chart in the report.
- Step 10** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.
- Step 11** In the **Email** text field, type in the email address where the generated report will be sent.
- Step 12** Click **Submit**.

Generating Web Reports on Demand

Most reports that you can schedule, you can also generate on demand.



Note Some reports are available only as Scheduled Reports, not on demand. See [Additional Extended Web Reports, on page 223](#).

To generate a report on demand, perform the following:

-
- Step 1** On the Security Management appliance, choose, **Web > Reporting > Archived Reports**.
- Step 2** Click on **Generate Report Now**.
- Step 3** From the **Report type** section, choose a report type from the drop-down list.
The options on the page may change.
- 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 raw 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** Depending on the options available for the report, choose:
- **Number of rows**: The number of rows of data to display in the table.
 - **Charts**: Which data to display in the chart(s) in the report:
 - Click the default option under Data to display.
 - **Sort Column**: The column to sort by for each table.
- Step 8** From the Delivery Option section, choose the following:
- If you want this report to appear on the Archived Reports page, select the **Archive Report** checkbox.
- 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 9** Click **Deliver This Report** to generate the report.
-

Archived Web Reports Page

- [About Scheduled and On-Demand Web Reports, on page 220](#)
- [Generating Web Reports on Demand , on page 224](#)
- [Viewing and Managing Archived Web Reports, on page 226](#)

Viewing and Managing Archived Web Reports

Use the information in this section to work with reports that are generated as scheduled reports.

My Web Reports under the Archive reports can only be seen by the user who created the Scheduled report.

-
- Step 1** Go to **Web > Reporting > Archived Reports**.
- Step 2** To view a report, click the report names in the Report Title column. The Show drop-down menu filters the types of reports that are listed on the **Archived Reports** page.
- Step 3** 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.
-

What to do next

Related Topics

- [Storage of Scheduled Web Reports](#) , on page 222
- [Adding Scheduled Web Reports](#), on page 222
- [Generating Web Reports on Demand](#) , on page 224

Schedule and Archive Web Reports on the New Web Interface

My Web Report is a user report under the Scheduled Reports menu. The user reports can only be seen by the user who has created them. My Web Reports under the Archive reports can only be seen by the user who created the Scheduled report.

- [Scheduling Web Reports on the New Web Interface](#), on page 226
- [Archiving Web Reports on the New Web Interface](#), on page 228

Scheduling Web Reports on the New Web Interface

This section includes the following:

- [Adding Scheduled Web Reports on the New Web Interface](#), on page 227
- [Editing Scheduled Web Reports on the New Web Interface](#), on page 227
- [Deleting Scheduled Web Reports on the New Web Interface](#), on page 228



Note You can choose to make user names unrecognizable in all reports. For information, see [Anonymizing User Names in Web Reports](#) , on page 166.

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 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.

Adding Scheduled Web Reports on the New Web Interface

- Step 1** On the Security Management appliance, choose **Web** from the Product drop-down. For more information, see [Using the Interactive Report Pages, on page 37](#).
- Step 2** Choose **Monitoring > Schedule & Archive**.
- Step 3** In the Scheduled / Archived tab, click the + button.
- Step 4** Select your report type from the **Report Type** drop-down menu.
- Step 5** In the **Report Title** field, enter the title of your report.
To avoid creating multiple reports with the same name, we recommend using a descriptive title.
- Step 6** Choose the time range for the report from the **Time Range to Include** drop-down menu.
- Step 7** Choose the format for the generated report.
The default format is PDF.
- Step 8** From the Delivery Options section, choose any one of the following:
By choosing this, the report will be listed on the Archived Reports page.
- Note** Domain-Based Executive Summary reports cannot be archived.
- To archive the report, select **Only Archive**.
 - To archive and email the report, click **Archive and Email to Recipients**.
 - To email the report, click **Only Email to Recipients**.
- In the **Email IDs** field, enter the recipient email addresses.
- Step 9** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.
- Step 10** Select the language in which the report must be generated from the **Report Language** drop-down list.
- Step 11** Click **Submit**.
-

Editing Scheduled Web Reports on the New Web Interface

To edit reports on the new web interface of your appliance, select **Web** from the Product drop-down and choose **Monitoring > Scheduled & Archive** page. Click on the link corresponding to the Report Title of reports that you want to edit. Modify settings then click **Edit** to submit your changes on the page.

Deleting Scheduled Web Reports on the New Web Interface

To delete reports on the new web interface of your appliance, select **Web** from the Product drop-down and choose **Monitoring > Scheduled / Archived** page. Select the checkboxes corresponding to the reports that you want to delete and click on the trash can icon.

To remove all scheduled reports, select the check box next to the report title. Note that archived versions of deleted reports are not deleted.

Archiving Web Reports on the New Web Interface

- [\[New Web Interface\] Generating Web Reports on Demand, on page 228](#)
- [Viewing and Managing Archived Web Reports on the New Web Interface, on page 229](#)

[New Web Interface] Generating Web Reports on Demand

Most reports that you can schedule, you can also generate on demand.



Note Some reports are available only as Scheduled Reports, not on demand. See [Additional Extended Web Reports, on page 223](#).

To generate a report on demand, perform the following:

-
- Step 1** On the Security Management appliance, select **Web** from the Product drop-down and choose **Monitoring > Schedule & Archive**.
 - Step 2** In the View Archived tab, click on the + button.
 - Step 3** From the **Report Type** section, choose a report type from the drop-down list.
The options on the page may change.
 - Step 4** In the **Report Title** section, enter 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 **Attachment Details** section, choose the format of the report.
PDF. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.
 - Step 7** From the **Delivery Options** section, choose any one of the following:
By choosing this, the report will be listed on the Archived Reports page.
 - Note** Domain-Based Executive Summary reports cannot be archived.
 - To archive the report, select **Only to Archive**.
 - To archive and email the report, click **Archive and Email to Recipients**.

- To email the report, click **Only Email to Recipients**.

In the **Email IDs** field, enter the recipient email addresses.

- Step 8** Select the language in which the report must be generated from the **Report Language** drop-down list.
- Step 9** Click **Deliver This Report** to generate the report.
-

Viewing and Managing Archived Web Reports on the New Web Interface

Use the information in this section to work with reports that are generated as scheduled reports.

- Step 1** Login to the new web interface of your appliance.
- Step 2** Choose **Web** from the Product drop-down and select **Monitoring > Schedule & Archive**.
- Step 3** Select the View Archived tab.
- Step 4** To view a report, click the report names in the Report Title column. The Report Type drop-down list filters the types of reports that are listed on the Archived Reports tab.
- Step 5** You can search for a particular report in the search box.
-

Web Tracking

Use the Web Tracking page to search for and view details about individual transactions or patterns of transactions that may be of concern. Depending on the services that your deployment uses, search in relevant tabs:

- [Searching for Transactions Processed by Web Proxy Services , on page 229](#)
- [Searching for Transactions Processed by the L4 Traffic Monitor , on page 233](#)
- [Searching for Transactions Processed by the SOCKS Proxy , on page 234](#)
- [Working with Web Tracking Search Results , on page 239](#)
- [Viewing Transaction Details for Web Tracking Search Results , on page 240](#)

Alternatively, use FQDN to search for website data on the Web Tracking page for some cases like Transparent Passthrough.

For more information about the distinction between the Web Proxy and the L4 Traffic Monitor, see the “Understanding How the Web Security Appliance Works” section in AsyncOS for Cisco Web Security Appliances User Guide.

Related Topics

- [About Web Tracking and Upgrades , on page 241](#)

Searching for Transactions Processed by Web Proxy Services

Use the **Proxy Services** tab on the **Web > Reporting > Web Tracking** page to search web tracking data aggregated from individual security components and acceptable use enforcement components. This data does not include L4 Traffic Monitoring data or transactions processed by the SOCKS Proxy.

You might want to use it to assist the following roles:

- **HR or Legal manager.** Run an investigative report for an employee during a specific time period.

For example, you can use the Proxy Services tab to retrieve information about a specific URL that a user is accessing, what time the user visited that URL, whether that URL is allowed, etc.

- **Network security administrator.** Examine whether the company network is being exposed to malware threats through employees' smartphones.

You can view search results for the transactions recorded (including blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.



Note The Web Proxy only reports on transactions that include an ACL decision tag other than "OTHER-NONE."

For an example of Web Tracking usage, see the [Example 1: Investigating a User](#), on page 625.

For an example of how the Proxy Services tab can be used with other web reporting pages, see the [Using The URL Categories Page in Conjunction with Other Reporting Pages](#), on page 177.

- Step 1** On the Security Management appliance, choose **Web > Reporting > Web Tracking**.
- Step 2** Click the **Proxy Services** tab.
- Step 3** To see all search and filtering options, click **Advanced**.
- Step 4** Enter search criteria:

Table 68: Web Tracking Search Criteria on the Proxy Services Tab

Option	Description
Default Search Criteria	
Time Range	Choose the time range on which to report. For information on time ranges available on the Security Management appliance, see the Choosing a Time Range for Reports , on page 26.
User/Client IPv4 or IPv6	Optionally, enter an authentication username as it appears in reports or a client IP address that you want to track. You can also enter an IP range in CIDR format, such as 172.16.0.0/16. When you leave this field empty, the search returns results for all users.
Website	Optionally, enter a website that you want to track. When you leave this field empty, the search returns results for all websites.
Transaction Type	Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.
Advanced Search Criteria	

Option	Description
URL Category	<p>To filter by a URL category, select Filter by URL Category and type the first letter of a custom or predefined URL category by which to filter. Choose the category from the list that appears . .</p> <p>If the set of URL categories has been updated, some categories may be labeled “Deprecated.” Deprecated categories are no longer being used for new transactions. However, you can still search for recent transactions that occurred while the category was active. For more information about URL category set updates, see URL Category Set Updates and Reports , on page 177.</p> <p>All recent transactions that match the category name are included, regardless of the engine name noted in the drop-down list.</p>
Application	<p>To filter by an application, select Filter by Application and choose an application by which to filter.</p> <p>To filter by an application type, select Filter by Application Type and choose an application type by which to filter.</p>
Policy	<p>To filter by a policy group, select Filter by Policy and enter a policy group name by which to filter.</p> <p>Make sure that you have declared the policy on the Web Security appliance.</p>
Malware Threat	<p>To filter by a particular malware threat, select Filter by Malware Threat and enter a malware threat name by which to filter.</p> <p>To filter by a malware category, select Filter by Malware Category and choose a malware category by which to filter. For descriptions, see Malware Category Descriptions, on page 181.</p>
WBRS	<p>In the WBRS section, you can filter by Web-Based Reputation Score and by a particular web reputation threat.</p> <ul style="list-style-type: none"> • To filter by web reputation score, select Score Range and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting No Score. • To filter by web reputation threat, select Filter by Reputation Threat and enter a web reputation threat by which to filter. <p>For more information on WBRS scores, see the IronPort AsyncOS for Web User Guide.</p>
AnyConnect Secure Mobility	<p>To filter by remote or local access, select Filter by User Location and choose an access type. To include all access types, select Disable Filter.</p> <p>(In previous releases, this option was labeled Mobile User Security.)</p>
Web Appliance	<p>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.</p> <p>If you select Disable Filter, the search includes all Web Security appliances associated with the Security Management appliance.</p>
User Request	<p>To filter by transactions that were actually initiated by the user, select Filter by Web User-Requested Transactions.</p> <p>Note: When you enable this filter, the search results include “best guess” transactions.</p>

Step 5 Click Search.**What to do next****Related Topics**

- [Displaying More Web Tracking Search Results](#) , on page 239
- [Understanding Web Tracking Search Results](#) , on page 239
- [Viewing Transaction Details for Web Tracking Search Results](#) , on page 240
- [About Web Tracking and Advanced Malware Protection Features](#) , on page 240

Malware Category Descriptions

The Web Security Appliance can block the following types of malware:

Malware Type	Description
Adware	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.
Browser Helper Object	A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	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.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	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.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Outbreak Heuristics	This category represents malware found by Adaptive Scanning independently of the other anti-malware engines.
Phishing URL	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.

Malware Type	Description
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following actions: Overtly or covertly records system processes and/or user action. 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 passphrases 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.

Searching for Transactions Processed by the L4 Traffic Monitor

The L4 Traffic Monitor tab on the **Web > Reporting > Web Tracking** page provides details about connections to malware sites and ports. You can search for connections to malware sites by the following types of information:

- Time range
- IP address of the machine that initiated the transaction (IPv4 or IPv6)
- Domain or IP address of the destination website (IPv4 or IPv6)
- Port
- IP address associated with a computer in your organization
- Connection type
- The Web Security appliance that processed the connection

The first 1000 matching search results are displayed.

To view the hostname at the questionable site or the Web Security appliance that processed the transaction, click the Display Details link in the Destination IP Address column heading.

For more information about how you can use this information, see [L4 Traffic Monitor Report](#), on page 189.

Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; IP address of the client machine that initiated the transaction; and destination domain, IP address, or port. You can also filter results by custom URL category, policy matched, and user location (local or remote). IPv4 and IPv6 addresses are supported.

-
- Step 1** Choose **Web > Reporting > Web Tracking**.
 - Step 2** Click the **SOCKS Proxy** tab.
 - Step 3** To filter results, click **Advanced**.
 - Step 4** Enter search criteria.
 - Step 5** Click **Search**.
-

What to do next

Related Topics

[SOCKS Proxy Report](#) , on page 191

Web Tracking on the New Web Interface

You can use the **Web Tracking Search** page to search and view details about individual transactions or patterns of transactions that may be of concern. Depending on the services that your deployment uses, search in relevant tabs:

- [Searching for Transactions Processed by Web Proxy Services](#) , on page 234
- [Searching for Transactions Processed by the L4 Traffic Monitor](#) , on page 233
- [Searching for Transactions Processed by the SOCKS Proxy](#) , on page 239
- [Working with Web Tracking Search Results](#) , on page 239
- [Viewing Transaction Details for Web Tracking Search Results](#) , on page 240

For more information about the distinction between the Web Proxy and the Layer4 Traffic Monitor, see the “Understanding How the Web Security Appliance Works” section in *User Guide for AsyncOS for Cisco Web Security Appliances*.

Searching for Transactions Processed by Web Proxy Services

You can use the **Proxy Services** tab on the **Web Tracking Search** page to search web tracking data aggregated from individual security components and acceptable use enforcement components. This data does not include Layer 4 Traffic Monitoring data or transactions processed by the SOCKS Proxy.

You might want to use it to assist the following roles:

- **HR or Legal manager.** Run an investigative report for an employee during a specific time period.

For example, you can use the Proxy Services tab to retrieve information about a specific URL that a user is accessing, what time the user visited that URL, whether that URL is allowed, etc.

- **Network security administrator.** Examine whether the company network is being exposed to malware threats through employees' smartphones.

You can view search results for the transactions recorded (including blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.



Note The Web Proxy only reports on transactions that include an ACL decision tag other than "OTHER-NONE."

For an example of Web Tracking usage, see the [Example 1: Investigating a User](#), on page 625.

For an example of how the Proxy Services tab can be used with other web reporting pages, see the [Using The URL Categories Page in Conjunction with Other Reporting Pages](#), on page 177.

- Step 1** On the Security Management appliance, choose **Web** from the dropdown list..
- Step 2** Choose **Tracking > Proxy Services**.
- Step 3** To see all search and filtering options, click **Advanced**.
- Step 4** Enter search criteria:

Table 69: Web Tracking Search Criteria on the Proxy Services Tab

Option	Description
Default Search Criteria	
Time Range	Choose the time range on which to report. For information on time ranges available on the Security Management appliance, see the Choosing a Time Range for Reports , on page 26.
User/Client IPv4 or IPv6	Optionally, enter an authentication username as it appears in reports or a client IP address that you want to track. You can also enter an IP range in CIDR format, such as 172.16.0.0/16. When you leave this field empty, the search returns results for all users.
Website	Optionally, enter a website that you want to track. When you leave this field empty, the search returns results for all websites.
Transaction Type	Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.
Advanced Search Criteria	

Option	Description
URL Category	<p>To filter by a URL category, select Filter by URL Category and type the first letter of a custom or predefined URL category by which to filter. Choose the category from the list that appears . .</p> <p>If the set of URL categories has been updated, some categories may be labeled “Deprecated.” Deprecated categories are no longer being used for new transactions. However, you can still search for recent transactions that occurred while the category was active. For more information about URL category set updates, see URL Category Set Updates and Reports , on page 177.</p> <p>All recent transactions that match the category name are included, regardless of the engine name noted in the drop-down list.</p>
Application	<p>To filter by an application, select Filter by Application and choose an application by which to filter.</p> <p>To filter by an application type, select Filter by Application Type and choose an application type by which to filter.</p>
Youtube (YT) Category	To filter by a specific Youtube category, expand the Youtube Category section and select the Youtube categories that you want to view.
Policy	<p>To filter by a policy group, select Filter by Policy and enter a policy group name by which to filter.</p> <p>Make sure that you have declared the policy on the Web Security appliance.</p>
Malware Threat	<p>To filter by a particular malware threat, select Filter by Malware Threat and enter a malware threat name by which to filter.</p> <p>To filter by a malware category, select Filter by Malware Category and choose a malware category by which to filter. For descriptions, see Malware Category Descriptions, on page 181.</p>
WBRS	<p>In the WBRS section, you can filter by Web-Based Reputation Score and by a particular web reputation threat.</p> <ul style="list-style-type: none"> To filter by web reputation score, select Score Range and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting No Score. To filter by web reputation threat, select Filter by Reputation Threat and enter a web reputation threat by which to filter. <p>For more information on WBRS scores, see the IronPort AsyncOS for Web User Guide.</p>
AnyConnect Secure Mobility	<p>To filter by remote or local access, select Filter by User Location and choose an access type. To include all access types, select Disable Filter.</p> <p>(In previous releases, this option was labeled Mobile User Security.)</p>
Web Appliance	<p>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.</p> <p>If you select Disable Filter, the search includes all Web Security appliances associated with the Security Management appliance.</p>

Option	Description
User Request	To filter by transactions that were actually initiated by the user, select Filter by Web User-Requested Transactions . Note: When you enable this filter, the search results include “best guess” transactions.

Malware Category Descriptions

The Web Security Appliance can block the following types of malware:

Malware Type	Description
Adware	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.
Browser Helper Object	A browser helper object is browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	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.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	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.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Outbreak Heuristics	This category represents malware found by Adaptive Scanning independently of the other anti-malware engines.
Phishing URL	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.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.

Malware Type	Description
System Monitor	A system monitor encompasses any software that performs one of the following actions: Overtly or covertly records system processes and/or user action. 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 passphrases 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.

Searching for Transactions Processed by the Layer 4 Traffic Monitor

The Layer 4 Traffic Monitor tab on the **Web Tracking Search** page provides details about connections to malware sites and ports. You can search for connections to malware sites by the following types of information:

- Time range
- IP address of the machine that initiated the transaction (IPv4 or IPv6)
- Domain or IP address of the destination website (IPv4 or IPv6)
- Port
- IP address associated with a computer in your organization
- Connection type
- The Web Security appliance that processed the connection

To view the hostname at the questionable site or the Web Security appliance that processed the transaction, click the Display Details link in the Destination IP Address column heading.

For more information about how you can use this information, see [Layer 4 Traffic Monitor Page, on page 201](#).

Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; IP address of the client machine that initiated the transaction; and destination domain, IP address, or port. You can also filter results by custom URL category, policy matched, and user location (local or remote). IPv4 and IPv6 addresses are supported.

-
- Step 1** On the Security Management appliance, choose **Web** from the dropdown list..
 - Step 2** Choose **Tracking > SOCKS Proxy**.
 - Step 3** To see all search and filtering options, click **Advanced**.
 - Step 4** Enter search criteria.
 - Step 5** Click **Search**.
-

What to do next

Related Topics

[SOCKS Proxy Report](#) , on page 191

Working with Web Tracking Search Results

- [Displaying More Web Tracking Search Results](#) , on page 239
- [Understanding Web Tracking Search Results](#) , on page 239
- [Viewing Transaction Details for Web Tracking Search Results](#) , on page 240
- [About Web Tracking and Upgrades](#) , on page 241

Displaying More Web Tracking Search Results

-
- Step 1** Be sure to review all pages of returned results.
 - Step 2** To display more results per page than the current number displayed, select an option from the **Items Displayed** menu.
 - Step 3** If more transactions match your criteria than the maximum number of transactions offered in the Items Displayed menu, you can view the complete set of results by clicking the **Printable Download** link to obtain a CSV file that includes all matching transactions.

This CSV file includes the complete set of raw data, excluding details of related transactions.

Understanding Web Tracking Search Results

By default, results are sorted by time stamp, with the most recent result at the top.

Search results include:

- The time that the URL was accessed.

- The number of related transactions spawned by the user-initiated transaction, such as images loaded, javascripts run, and secondary sites accessed. The number of related transactions appears in each row below the Display All Details link in the column heading.
- The disposition (The result of the transaction. If applicable, shows the reason the transaction was blocked, monitored, or warned.)

Viewing Transaction Details for Web Tracking Search Results

To View	Do This
The full URL for a truncated URL in the list	Note which host Web Security Appliance processed the transaction, then check the Accesslog on that appliance.
Details for an individual transaction	Click a URL in the Website column.
Details for all transactions	Click the Display All Details... link in the Website column heading.
A list of up to 500 related transactions	The number of related transactions appears in parentheses below the "Display Details" link in the column heading in the list of search results. Click the Related Transactions link in the Details view for a transaction.

About Web Tracking and Advanced Malware Protection Features

When searching for file threat information in Web Tracking, keep the following points in mind:

- To search for malicious files found by the file reputation service, select **Known Malicious and High-Risk Files** for the **Filter by Malware Category** option in the Malware Threat area in the Advanced section in Web Tracking.
- Web Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a transaction was processed. For example, if a file was initially found to be clean, then a verdict update found the file to be malicious, only the clean verdict appears in Tracking results.

"Block - AMP" in search results means the transaction was blocked because of the file's reputation verdict.

In Tracking details, the "AMP Threat Score" is the best-effort score that the cloud reputation service provides when it cannot determine a clear verdict for the file. In this situation, the score is between 1 and 100. (Ignore the AMP Threat Score if an AMP Verdict is returned or if the score is zero.) The appliance compares this score to the threshold score (configured on the Security Services > Anti-Malware and Reputation page) to determine what action to take. By default, files with scores between 60 and 100 are considered malicious. Cisco does not recommend changing the default threshold score. The WBRS score is the reputation of the site from which the file was downloaded; this score is not related to the file reputation.

- Verdict updates are available only in the AMP Verdict Updates report. The original transaction details in Web Tracking are not updated with verdict changes. To see transactions involving a particular file, click a SHA-256 in the verdict updates report.

- Information about File Analysis, including analysis results and whether or not a file was sent for analysis, are available only in the File Analysis report.

Additional information about an analyzed file may be available from the cloud. To view any available File Analysis information for a file, select **Reporting > File Analysis** and enter the SHA-256 to search for the file, or click the SHA-256 link in Web Tracking details. If the File Analysis service has analyzed the file from any source, you can see the details. Results are displayed only for files that have been analyzed.

If the appliance processed a subsequent instance of a file that was sent for analysis, those instances will appear in Web Tracking search results.

Related Topics

- [Identifying Files by SHA-256 Hash](#) , on page 184

About Web Tracking and Upgrades

New web tracking features may not apply to transactions that occurred before upgrade, because the required data may not have been retained for those transactions. For possible limitations related to web tracking data and upgrades, see the Release Notes for your release.

Troubleshooting Web Reporting and Tracking

- [Centralized Reporting Is Enabled Properly But Not Working](#) , on page 241
- [Advanced Malware Protection Verdict Updates Report Results Differ](#) , on page 241
- [Issues Viewing File Analysis Report Details](#) , on page 242
- [Expected Data Is Missing from Reporting or Tracking Results](#), on page 242
- [PDF Shows Only a Subset of Web Tracking Data](#) , on page 243
- [Troubleshooting L4 Traffic Monitor Reports](#) , on page 243
- [Exported .CSV file is Different From Web Interface Data](#) , on page 243

See also [Troubleshooting All Reports](#) , on page 33.

Centralized Reporting Is Enabled Properly But Not Working

Problem

You have enabled centralized web reporting as directed, but it is not working.

Solution

If there is no disk space allocated for reporting, 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 Space](#) , on page 521, for more information.

Advanced Malware Protection Verdict Updates Report Results Differ

Problem

A Web Security appliance and an Email Security appliance sent the same file for analysis, and the AMP Verdict Updates reports for Web and Email show different verdicts for that file.

Solution

This situation is temporary. Results will match once all verdict updates have been downloaded. Allow up to 30 minutes for this to occur.

Issues Viewing File Analysis Report Details

- [File Analysis Report Details Are Not Available](#) , on page 242
- [Error When Viewing File Analysis Report Details](#), on page 242

File Analysis Report Details Are Not Available

Problem

File Analysis report details are not available.

Solution

See [Requirements for File Analysis Report Details](#) , on page 183.

Error When Viewing File Analysis Report Details

Problem

No cloud server configuration is available, error appears when you attempt to view File Analysis report details.

Solution

Go to **Management Appliance > Centralized Services > Security Appliances** and add at least one Web Security appliance that has the File Analysis feature enabled.

Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance

Problem

You see an API key, registration, or activation error when attempting to view File Analysis report details.

Solution

If you are using a private cloud (on-premises) Cisco AMP Threat Grid appliance for file analysis, see [\(On-Premises File Analysis\) Activate the File Analysis Account](#) , on page 184.

If your Threat Grid appliance hostname changes, you must repeat the process in the referenced procedure.

Expected Data Is Missing from Reporting or Tracking Results

Problem

Expected data is missing from reporting or tracking results.

Solution

Possible causes:

- Make sure you have selected the desired time range.
- For tracking results, be sure you are viewing all matching results. See [Displaying More Web Tracking Search Results](#) , on page 239.
- Data transfer between Web Security appliances and the Cisco Secure Email and Web Manager appliance may have been interrupted, or data may have been purged. See [Data Availability Page](#) , on page 194.
- If an upgrade changes the way information is reported or tracked, transactions that occurred before upgrade may not be represented as expected. To see if your release has this type of change, see the Release Notes for your release at the location specified in [Documentation](#) , on page 629.
- For missing results in Web Proxy Services tracking search results, see [Searching for Transactions Processed by Web Proxy Services](#) , on page 229.
- For unexpected results when filtering by user requested transactions, see the User Request row of the table in [Searching for Transactions Processed by Web Proxy Services](#) , on page 229.

PDF Shows Only a Subset of Web Tracking Data

Problem

PDF shows only some of the data that is visible on the Web Tracking page.

Solution

For information about what data is included in and omitted from PDFs and CSV files, see the web tracking information in the table in [Exporting Reporting and Tracking Data](#) , on page 31.

Troubleshooting L4 Traffic Monitor Reports

If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy's data port is recorded and displayed as the client IP address in reports. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses. To do this, see the IronPort AsyncOS for Web User Guide.

Related Topics

- [Client Malware Risk Report](#) , on page 187
- [Searching for Transactions Processed by the L4 Traffic Monitor](#) , on page 233

Exported .CSV file is Different From Web Interface Data

Problem

Domains Matched data exported to .csv file differs from the data shown in the Web interface.

Solution

For performance reasons, only the first 300,000 entries are exported as .csv.

Issues Exporting Web Tracking Search Results

Problem

Web tracking search results display an “Out of Memory” errors when you simultaneously run multiple large search queries.

Solution

You can increase the heap size of the memory to 1024 MB or more or reduce the time range of your search criteria as a workaround. Keep in mind that increasing the heap size of the memory can cause memory-related issues.



CHAPTER 7

FIPS Management

This chapter contains the following sections:

- [FIPS Management Overview, on page 245](#)
- [Configuration Changes in FIPS Mode, on page 245](#)
- [Switching the Appliance to FIPS Mode, on page 246](#)
- [Checking FIPS Mode Compliance, on page 247](#)

FIPS Management Overview

The Federal Information Processing Standard (FIPS) 140 is a publicly announced standard developed jointly by the United States and Canadian federal governments specifying requirements for cryptographic modules that are used by government agencies to protect sensitive but unclassified information. The Cisco Secure Email and Web Manager uses the CiscoSSL Cryptographic Toolkit to achieve FIPS 140-2 Level 1 compliance.

The CiscoSSL Cryptographic Toolkit is a GCT-approved cryptography suite that includes CiscoSSL, which is an enhanced version of OpenSSL's FIPS support, and the FIPS-compliant Cisco Common Cryptography Module. The Cisco Common Cryptography Module is a software library that Secure Email and Web Manager uses for FIPS-validated cryptographic algorithms for protocols such as SSH and TLS.



Note The Cisco Secure Email and Web Manager FIPS Certification only applies to email gateway integration and not to Secure Web Appliance integration.

Configuration Changes in FIPS Mode

The Secure Email and Web Manager uses Cisco SSL and FIPS-compliant certificates for communication when the appliance is in FIPS mode. See [Switching the Appliance to FIPS Mode, on page 246](#) for more information.

To be FIPS Level 1 compliant, the Secure Email and Web Manager makes the following changes to your configuration:

- **SMTP receiving and delivery:** Incoming and outgoing SMTP conversations over TLS between a public listener on the Secure Email and Web Manager and a remote host use TLS version 1.1 or 1.2 and FIPS cipher suites. TLS v 1.1 and 1.2 are the version of TLS supported in FIPS mode.

- **Web interface:** HTTPS sessions to the Secure Email and Web Manager's web interface use TLS version 1.1 or 1.2 and FIPS cipher suites. This also includes HTTPS sessions to the Spam Quarantine and other IP interfaces.
- **LDAPS:** TLS transactions between the Secure Email and Web Manager and LDAP servers, including using an LDAP server for external authentication, use TLS version 1.1 or 1.2 and FIPS cipher suites. If the LDAP server uses MD5 hashes to store passwords, the SMTP authentication query will fail because MD5 is not FIPS-compliant.
- **Logs:** SSH2 is the only allowed protocol for pushing logs via SCP. For error messages related to FIPS management, read the FIPS Logs at the INFO level.
- **SSL Ciphers:** Only the FIPS compliant SSL ciphers are supported.

Switching the Appliance to FIPS Mode

Use the `fipsconfig` CLI command to switch the appliance over to FIPS mode.



Note Only administrators can use this command. A reboot is required after switching the appliance from non-FIPS mode to FIPS mode.

Before You Begin

Make sure that the appliance do not have any objects that are not FIPS compliant. To enable FIPS mode, you must modify all the non-FIPS-compliant objects to meet FIPS requirements. See [Configuration Changes in FIPS Mode, on page 245](#). For instructions to check if your appliance contains non-FIPS-compliant objects, see [Checking FIPS Mode Compliance, on page 247](#).

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[ ]> setup
```

In FIPS mode, the RSA certificates must have 2048 bits or more key length, and the MD5 algorithm is deprecated.
 It is not recommended to add WSA (in FIPS or non-FIPS mode) to an SMA in FIPS Mode.
 It is not recommended to add ESA in non-FIPS mode to an SMA in FIPS Mode.
 It is not recommended to move SMA to FIPS Mode when the connected ESA or WSA is in non-FIPS mode.

```
To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to enable FIPS mode and reboot now ? [N]> y
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System rebooting. Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

Checking FIPS Mode Compliance

Use the `fipsconfig` command to check if your Secure Email and Web Manager contains any non-FIPS-compliant objects.

Procedure

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> fipscheck
All objects in the current configuration are FIPS compliant.
FIPS mode is currently disabled.
```




CHAPTER 8

Tracking Messages

This chapter contains the following sections:

- [Tracking Service Overview](#), on page 249
- [Setting Up Centralized Message Tracking](#), on page 250
- [Checking Message Tracking Data Availability](#), on page 253
- [Searching for Email Messages](#), on page 253
- [Understanding Tracking Query Results](#), on page 261
- [Troubleshooting Message Tracking](#), on page 264
- [Exporting Message Service](#), on page 265

Tracking Service Overview

The tracking service of the Cisco Secure Email and Web Manager 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:

- **Time Frame:** Find a message that was sent between specified dates and times.
- **Envelope Information:** Find messages from particular envelope senders or recipients by entering the text strings to match.
- **Subject:** Match a text string in the subject line. Warning: Do not use this type of search in environments where regulations prohibit such tracking.
- **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.
- **File SHA256:** Find messages with the SHA-256 value of the message file
- **Cisco Host:** Narrow search criteria to particular Email Security appliances, or search across all managed appliances.
- **Message ID Header and Cisco MID:** Find messages by identifying the SMTP “Message-ID:” header or the Cisco message ID (MID).
- **Sender IP Address/ Domain/ Network Owner:** Search for messages from a particular IP address, domain name or network owner.
- **Message 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
- **Rejected Connections:** Search for messages from a particular IP address, domain name or network owner of the rejected connections in the search results

Setting Up Centralized Message Tracking

To set up centralized message tracking, complete the following procedures in order:

1. [Enabling Centralized Email Tracking, on page 250](#)
2. [Configuring Centralized Message Tracking on Email Security Appliances , on page 251](#)
3. [Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance , on page 252](#)

Enabling Centralized Email Tracking

- [Enabling Centralized Email Tracking on the Legacy Web Interface, on page 251](#)
- [Enabling Centralized Email Tracking on the New Web Interface, on page 251](#)


Enabling Centralized Email Tracking on the Legacy Web Interface

- Step 1** Choose **Management Appliance > Centralized Services > Email > Centralized Message Tracking**.
 - Step 2** In the Message Tracking Service section, click **Enable**.
 - Step 3** 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**.
 - Step 4** Submit and commit your changes.
-

What to do next

[Configuring Centralized Message Tracking on Email Security Appliances , on page 251](#)


Enabling Centralized Email Tracking on the New Web Interface

- Step 1** On the Security Management appliance, click **Service Status** and hover over the  corresponding to **Message Tracking** card.
 - Step 2** Click **Edit Settings**.
 - Step 3** If you are enabling centralized email tracking for the first time after running the System Setup Wizard, review and accept the license agreement, and click **Proceed**.
 - Step 4** Click the toggle switch to enable Centralized Email Tracking.
 - Step 5** Select the appropriate fields and click **Submit**.
-

What to do next

[Configuring Centralized Message Tracking on Email Security Appliances , on page 251](#)

Configuring Centralized Message Tracking on Email Security Appliances

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Verify that Message Tracking is configured and working properly on the Email Security appliance.
- Step 3** Go to **Security Services > Message Tracking**.
- Step 4** Click **Edit Settings**.
- Step 5** Select **Centralized Tracking**.
- Step 6** Click **Submit**.
- Step 7** If you want to be able to search for and log the names of email attachments:

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 the documentation or online help for your Email Security appliance.


- Step 8** Submit and commit your changes.
- Step 9** Repeat for each Email Security appliance to manage.

What to do next

[Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance](#), on page 252

Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance

The steps you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** If you have already added the Email Security appliance to the list on this page:
- Click the name of an Email Security appliance.
 - Select the **Centralized Message Tracking** service.
- Step 4** If you have not yet added the Email Security appliance:
- Click Add Email Appliance.
 - In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Email Security appliance.
- Note** If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.
- The Centralized Message Tracking service is pre-selected.
 - Click **Establish Connection**.
 - Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.
- 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.
- Wait for the Success message to appear above the table on the page.
 - Click **Test Connection**.
 - Read test results above the table.
- Step 5** Submit and commit your changes.
- Step 6** Repeat this procedure for each Email Security appliance for which you want to enable Centralized Message Tracking.
-

Managing Access to Sensitive Information

If you will distribute administrative tasks to other people and you want to restrict their access to sensitive information that may appear in email messages that violate Data Loss Prevention (DLP) policies, see [Controlling Access to Sensitive Information in Message Tracking](#), on page 430.

Checking Message Tracking Data Availability

You can determine the date range that your message tracking data includes, as well as identify any missing intervals in that data.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Email > Message Tracking > Message Tracking Data Availability**.
-

Searching for Email Messages



Note After upgrading to AsyncOS 13.6.1, the state of the messages that were in quarantine prior to the upgrade does not change.

- [Searching for Email Messages on the New Web Interface, on page 253](#)
- [Searching for Email Messages on the Legacy Web Interface, on page 255](#)
- [Remediating Messages in Mailboxes, on page 257](#)

Searching for Email Messages on the New Web Interface

The tracking service of the appliance lets you 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, or processing event (for example, whether the message was virus positive, spam positive, hard bounced, delivered, and so forth). Message tracking gives you 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.

-
- Step 1** On the Security Management appliance, choose **Tracking > Search**.
- Step 2** Select **Messages** tab or **Rejected Connections** tab to narrow your search results.

Note You can search for rejected connections based on the sender IP address, domain or network owner.

Step 3 (Optional) Click the **Advanced Search** to display additional search options.

Step 4 Enter the following search criteria:

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

- [For Messages and Rejected Connections] **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.

- **Envelope Sender:** Select Begins With, Is, or Contains, and enter a text string to search for in the envelope sender. You can enter email addresses, user names, or domains. Use the following formats:
 - For email domains: *example.com*, *[203.0.113.15]*, *[ipv6:2001:db8:80:1::5]*
 - For full email addresses: *user@example.com*, *user@[203.0.113.15]* or *user@[ipv6:2001:db8:80:1::5]*.
 - You can enter any character(s). No validation of your entry is performed.

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

- **Envelope Recipient:** Select Begins With, Is, or Contains, and enter text to search for in the envelope recipient. You can enter email addresses, user names, or 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.

Otherwise, valid search criteria for Envelope Recipient are the same as those for Envelope Sender.

You can enter any character(s). No validation of your entry is performed.

- **Attachment Name:** Select Begins With, Is, or Contains, and enter an ASCII or Unicode text string for one Attachment Name to find. Leading and trailing spaces are not stripped from the text you enter.
- **Reply-To:** Select Begins With, Is, or Contains, and enter a text string to search for messages based on the Reply-To header of the message.
- **File SHA256:** Enter a File SHA-256 value of the message.

For more information about identifying files based on SHA-256 hash, see [Identifying Files by SHA-256 Hash](#), on page 84.

- **Cisco Host:** Select All Host to search across all email security appliances or select the required email security appliance from the drop-down menu.
- **Message ID Header and Cisco MID:** Enter a text string for the message ID header, the Cisco IronPort message ID (MID), or both.
- [For Messages and Rejected Connections] **Sender IP Address/ Domain/ Network Owner:** Enter a sender IP address, domain or network owner details.
 - An IPv4 address must be 4 numbers separated by a period. Each number must be a value from 0 to 255. (Example: 203.0.113.15).
 - An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons. You can use zero compression in one location, such as 2001:db8:80:1::5.
- **Message Event:** Select the events to track. Options are Virus Positive, Spam Positive, Suspect Spam, contained malicious URLs, contained URL in specified category, DLP Violations (you can enter the name of a DLP policy and select violation severities or action taken), DMARC violations, Delivered, Advanced Malware Protection Positive (for malware found in an attachment), Hard Bounced, Soft Bounced, currently in a policy, virus, or outbreak quarantine, caught by message filters or content filters, 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.

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.

Note In the new web interface, to perform a partial URL search, you need to add "*" before and after the search string to retrieve the results.

Step 5 Click Search.

Each row corresponds to an email message. Scroll down to load more messages in the view.

If necessary, you can refine your 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.

Click Export to export the search results.

What to do next

- [Narrowing the Result Set, on page 259](#)
- [About Message Tracking and Advanced Malware Protection Features , on page 260](#)
- [Understanding Tracking Query Results, on page 261](#)

Searching for Email Messages on the Legacy Web Interface

The Security Management appliance’s tracking service lets you 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, or processing event (for example, whether the message was virus positive, spam positive, hard bounced, delivered, and so forth). Message tracking gives you 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.

Step 1 Choose **Email > Message Tracking > Message Tracking**.

Step 2 (Optional) Click the Advanced link to display more search options.

Step 3 Enter search criteria:

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

- Envelope Sender: Select Begins With, Is, or Contains, and enter a text string to search for in the envelope sender. You can enter email addresses, user names, or domains. Use the following formats:
 - For email domains: example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]
 - For full email addresses: user@example.com, user@[203.0.113.15] or user@[ipv6:2001:db8:80:1::5].
 - You can enter any character(s). No validation of your entry is performed.
- Envelope Recipient: Select Begins With, Is, or Contains, and enter text to search for in the envelope recipient. You can enter email addresses, user names, or 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.

Otherwise, valid search criteria for Envelope Recipient are the same as those for Envelope Sender.

You can enter any character(s). No validation of your entry is performed.

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

- An IPv4 address must be 4 numbers separated by a period. Each number must be a value from 0 to 255. (Example: 203.0.113.15).
- An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons. You can use zero compression in one location, such as 2001:db8:80:1::5.
- Message Event: Select the events to track. Options are Virus Positive, Spam Positive, Suspect Spam, contained malicious URLs, contained URL in specified category, DLP Violations (you can enter the name of a DLP policy and select violation severities or action taken), DMARC violations, Delivered, Advanced Malware Protection Positive (for malware found in an attachment), Hard Bounced, Soft Bounced, currently in a policy, virus, or outbreak quarantine, caught by message filters or content filters, Macro File Types Detected, Geolocation, Low Risk 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. Leading and trailing spaces are not stripped from the text you enter.

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 4 Click Search.

The query results appear at the bottom of the page. Each row corresponds to an email message.

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.

What to do next

- [Narrowing the Result Set, on page 259](#)
- [About Message Tracking and Advanced Malware Protection Features , on page 260](#)
- [Understanding Tracking Query Results, on page 261](#)

Remediating Messages in Mailboxes

Cisco Secure Email and Web Manager appliance provides the capability to remediate the malicious messages that are already delivered to the user mailbox. You can configure your appliance to remediate the messages by using the Message Tracking filter.

You can perform remedial actions manually on messages that are already delivered to the user mailbox. For example, an administrator monitoring the incoming messages can perform remedial actions on messages in the user mailbox using the Message Tracking filter.

You can also use the Message Tracking page to search and remediate the messages that are delivered to the user mailbox. The Message Tracking page is a unified place to search for all messages delivered to the mailboxes. From the search result, you can choose the messages you want to remediate and apply the action you want to perform on the messages.

Search and Remediate Messages Workflow

1. Message reaches the appliance and is delivered to the recipient.
2. The user searches for the message delivered to the recipient using the Message Tracking filter.
3. The user selects the message to be remediated from the recipient's mailbox and applies the remedial action on the message.

Search and Remediate Actions on Messages in the Mailboxes

Before you begin

- Make sure that you have enabled mailbox remediation and configured the account settings on Cisco Email Security Gateway.
- Enable Message Tracking on your appliance. See [Setting Up Centralized Message Tracking](#), on page 250.
- If you are using the Centralized Message Tracking service, make sure that you have enabled the trailblazer port and AsyncOS API HTTP port on the managed Cisco Email Security Gateway and the Cisco Secure Email and Web Manager appliance can access the trailblazer port. If the trailblazer port is disabled, ensure that the Cisco Secure Email and Web Manager appliance can access the AsyncOS API HTTP(S) port on the managed Cisco Email Security Gateway.
- If the managed Cisco Email Security appliance is using a certificate whose Certificate Authority does not exist in the Cisco Secure Email and Web Manager appliance trust store, the server certificate validation on the Content Security Management appliance fails. To allow communication, add the Certificate Authority of the signed certificate used by the Cisco Email Security appliance to the Cisco Secure Email and Web Manager appliance. To add the Certificate Authority, use `certconfig > CERTAUTHORITY` sub command in the CLI.

CAUTION: If you want to disable the server certificate validation on the Secure Email and Web Manager appliance, use the `esaapiconfig` command in the CLI. Cisco does not recommend you to disable the certificate validation for security reasons.

-
- Step 1** On the Security Management appliance, click on the **Tracking** tab on the new web interface of the appliance.
- Step 2** Click the **Messages** tab to narrow your search results. For more information, see [Searching for Email Messages on the New Web Interface](#), on page 253.
- Step 3** Select the messages you want to remediate. You can select a maximum of 1000 messages at a time. You can remediate the messages that are only in the delivered state.
- Step 4** Click **Remediate**.
- Step 5** Enter the following details:

- Enter a batch name for the remediation.
- Select anyone of the following remediation action:
 - Delete the messages. Select this option to permanently delete the messages from the end user's mailbox.
 - Forward to an email address. Select this option to forward the messages to a specified user, for example, an email administrator.
 - Forward to an email address and delete the messages. Select this option to forward the messages to a specified user, for example, an email administrator and permanently delete that messages from the end user's mailbox.

Step 6 Click **Apply**.

After you click **Apply**, you can view the Remediation Report Status widget at the bottom-right corner of the Message Tracking page. Use this widget to check the status of the Remediation Report generation. After the Remediation Report generation is complete, click View Details on the widget to go to the Remediation Report to view the remediation results.

Note You can also view Remediation Report directly by navigating to **Reports > User Reports >> Remediation Report** and click the Mailbox Search And Remediate tab.

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.

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 [New Web Interface Only] In the Message Tracking search criteria, click **Modify**.

Use the following parameter values to refine the search:

- Date and time
- Message ID (MID)
- Cisco Host (the Email Security appliance)
- Sender

- Recipient
- The subject line of the message, or starting words of the subject
- Message Event
- Additional Details (Message Last State, SBRS, Sender IP, and Group)

Step 3 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 4 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.

About Message Tracking and Advanced Malware Protection Features

When searching for file threat information in Message Tracking, keep the following points in mind:

- To search for malicious files found by the file reputation service, select **Advanced Malware Protection Positive** for the Message Event option in the Advanced section in Message Tracking.
- Message Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a message was processed. For example, if a file was initially found to be clean, then a verdict update found the file to be malicious, only the clean verdict appears in Tracking results.

In Message Tracking details, the Processing Details section shows:

- The SHA-256 of each attachment in the message, and
- The final Advanced Malware Protection verdict for the message as a whole, and
- Any attachments which were found to contain malware.

No information is provided for clean or unscannable attachments.

- Verdict updates are available only in the AMP Verdict Updates report. The original message details in Message Tracking are not updated with verdict changes. To see messages that have a particular attachment, click a SHA-256 in the verdict updates report.
- Information about File Analysis, including analysis results and whether or not a file was sent for analysis, are available only in the File Analysis report.

Additional information about an analyzed file may be available from the cloud. To view any available File Analysis information for a file, select **Monitor > File Analysis** and enter the SHA-256 to search for the file. If the File Analysis service has analyzed the file from any source, you can see the details. Results are displayed only for files that have been analyzed.

If the appliance processed a subsequent instance of a file that was sent for analysis, those instances will appear in Message Tracking search results.

Understanding Tracking Query Results

If results are not what you expected, see [Troubleshooting Message Tracking, on page 264](#).

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

To view detailed information about a message, click the **More Details** link in the new web interface or **Show Details** link in the legacy web interface, for that message. For more information, see the [Message Details, on page 261](#).



Note

- Messages with 50 or more recipients will not appear in tracking query results. This issue will be resolved in a future release.
- [New Web Interface Only] You can scroll down to display the search results when you specify your query. More results are displayed in the view as you scroll down.
- You can export the search results to a .csv file using the **Export** link above the search results section. You can choose to display up to 1000 search results when you specify your query. To view up to 50,000 messages that match your criteria, click the **Export All** link above the search results section and open the resulting .csv file in another application.
- If you clicked a link in a report page to view message details in Message Tracking, and the results are unexpected, this can occur if reporting and tracking were not both simultaneously and continuously enabled during the time period you are reviewing.
- For information about printing or exporting message tracking search results, see [Exporting Reporting and Tracking Data , on page 31](#).

Related Topics

[Message Details, on page 261](#)

Message Details

To view detailed information about a particular email message, including the message header information and processing details, click **More Details** link for any item in the search results list. A new window opens with the message details.

The message details include the following sections:

- [Verdict Chart and Last State Verdicts, on page 262](#)
- [Envelope and Header Summary, on page 263](#)
- [Sending Host Summary, on page 263](#)
- [Processing Details, on page 263](#)

Verdict Chart and Last State Verdicts

A Verdict Chart displays information of the various possible verdicts triggered by each engine of the email security appliance.



Note Verdict charts for AsyncOS prior to 12.0 will not be displayed and last state verdicts is displayed as "Last State Not Available".

The following table shows the various verdicts of each engine:

Table 70: Verdict Charts

Connection Behavior	Message Filter	Anti-Spam	Anti-Virus	AMP	Graymail	Content Filter	Outbreak Filter	DLP
Not Applicable	Not Evaluated	Not Evaluated	Not Evaluated	Not Evaluated	Not Evaluated	Not Evaluated	Not Evaluated	Not Evaluated
Accepted	Match	Negative	Negative	Clean	Negative	Match	Match	No Trigger
Relayed	No Match	Suspect	Repaired	FA	Positive	No Match	No Match	Violation
		Bulk Mail	Encrypted	Pending				No Violation
		Social Mail	Unscannable	Unknown				No Violation
		Marketing Mail	Positive	Skipped				No Violation
		Positive		Malicious				No Violation
				Unscannable				No Violation
				Low Risk				No Violation

The Last State verdict of the message determines the final verdict that is triggered after all the possible verdicts of each of the engine in your appliance.

Following are some of the last state verdicts:

- **Delivered:** When a message is delivered.
- **Dropped:** When a message is dropped.
- **Aborted:** When a message is aborted. (Example: Due to Mail Policy restrictions)
- **Bounced:** When a message is bounced back.
- **Splintered:** When the MID of a message is split into multiple MIDs having multiple final states.
- **Quarantined:** When a message is quarantined by engines.
- **Queued:** When a message is queued for delivery either to end recipient or to an off-box Spam quarantine or Centralized Policy, Virus or Outbreak quarantine.
- **Processing:** When a message is not completely processed by all the engines; or when a message is waiting in a queue of a particular engine.
- **Last State Not Available:** When last state of message cannot be retrieved. (Example: When message is still being processed by the engine and has not reached any final state.

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 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.

Sender Group: The sender group that received the message.

Message Size: The size of the message.

Policy Match (Incoming or Outgoing): The policy that received the message.



Note If the engine is not able to fetch the details, the value is displayed as “N/A”.

Sending Host Summary

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

IP Address: IP address of the sending host.

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

Processing Details

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

Entries include information about mail policy processing, such as anti-spam and anti-virus scanning, and other events such as message splitting.

If the message was delivered, the details of the delivery appear here. For example, a message may have been delivered and a copy kept in quarantine.

The last recorded event is highlighted in the processing details.

Summary Tab

This tab displays the summary logs of all the events during the processing of message.

DLP Matched Content Tab

This tab 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 have access, but not Administrator-level access, to the Security Management appliance. See [Controlling Access to Sensitive Information in Message Tracking](#), on page 430.

URL Details Tab

This tab displays only for messages caught by URL Reputation and URL Category content filters and by outbreak filters not message filters.

This tab displays the following information:

- The reputation score or category associated with the URL
- The action performed on the URL (rewrite, defang, or redirect)
- If a message contains multiple URLs, which URL has triggered the filter action.

You can see this tab only if you have configured your Email Security appliance to display this information. See *User Guide for AsyncOS for Cisco Email Security Appliances*.

To control access to this tab, see [Controlling Access to Sensitive Information in Message Tracking](#), on page 430

SMTP Log Tab

This section displays a log of messages when the sender of the email fails SMTP authentication.

AMP Log Tab

This section displays a log of messages caught by the Advanced Malware Protection file reputation and file analysis service.

Troubleshooting Message Tracking

- [Expected Messages Are Missing from Search Results](#), on page 264
- [Attachments Do Not Appear in Search Results](#), on page 265

Expected Messages Are Missing from Search Results

Problem

Search results did not include messages that should have met the criteria.

Solution

- Results for many searches, especially Message Event searches, depend on your appliance configuration. For example, if you search for a URL Category for which you have not filtered, no results will be found, even if a message contains a URL in that category. Verify that you have configured the Email Security

appliance properly to achieve the behavior that you expected. For example, check your mail policies, content and message filters, and quarantine settings.

- See [Checking Message Tracking Data Availability](#) , on page 253.

Attachments Do Not Appear in Search Results

Problem

Attachment names are not found and displayed in search results.

Solution

At least one incoming content filter or other body scanning feature configured and enabled on the ESA. See configuration requirements at [Enabling Centralized Email Tracking on the Legacy Web Interface, on page 251](#) and limitations for attachment name searches in [Tracking Service Overview](#).

Exporting Message Service

You can view additional fields to perform analysis and investigation on related mails using the Export file option along with messages.

Step 1 Choose **Tracking > Messages**.

Step 2 Select your criteria.

Step 3 Click **Export**.

You can view additional fields to perform analysis and investigation on related mails using the Export file option along with the message. The additional fields you can view include:

- Message Size- The size of the message.
 - Attachment Details- The name of the files attached to the message.
 - Delivery Details- Delivery information, such as the number of messages from a particular domain that were bounced.
 - Source IP/FQDN- The IP address of the sender.
 - Sender Group- The sender group that received the message.
 - DKIM, SPF, or DMARC Status- Authentication method to verify if the email was actually sent by the owner.
 - URL List- Cisco Secure Email and Web Manager displays only 1024 characters of the URL.
-



CHAPTER 9

Spam Quarantine

This chapter contains the following sections:

- [Overview of the Spam Quarantine](#) , on page 267
- [Local Versus External Spam Quarantine](#) , on page 267
- [Setting Up the Centralized Spam Quarantine](#) , on page 268
- [Edit Spam Quarantine Page](#) , on page 276
- [Using Safelists and Blocklists to Control Email Delivery Based on Sender](#) , on page 276
- [Configuring Spam Management Features for End Users](#) , on page 287
- [Managing Messages in the Spam Quarantine](#) , on page 299
- [Disk Space for the Spam Quarantine](#) , on page 301
- [About Disabling the External Spam Quarantine](#) , on page 301
- [Troubleshooting Spam Quarantine Features](#) , on page 302

Overview of the Spam Quarantine

The Spam Quarantine (also known as ISQ) and End-User Quarantine (also known as EUQ) provides a safeguard mechanism for organizations that are concerned about “false positives” — that is, legitimate email messages that the appliance has deemed to be spam. When the appliance determines that a message is spam or suspected spam, you may want to let the recipient or an administrator review the message before delivering or deleting it. The spam quarantine stores messages for this purpose.

Administrative users of the appliance can view all messages in a spam quarantine. End users, usually the message recipients, can view their own quarantined messages in a slightly different web interface.

The spam quarantine is separate from policy, virus, and outbreak quarantines.

Related Topics

- [Centralized Policy, Virus, and Outbreak Quarantines](#), on page 303

Local Versus External Spam Quarantine

A local spam quarantine stores spam and suspect spam on the appliance . An external spam quarantine can store these messages on a separate Cisco Content Security Management appliance .

Consider using an external spam quarantine if:

- You want a centralized location to store and manage spam from multiple appliances .
- You want to store more spam than the appliance can hold.
- You want to regularly back up the spam quarantine and its messages.

Setting Up the Centralized Spam Quarantine

Procedure

	Command or Action	Purpose
Step 1	On the Security Management appliance, enable the centralized spam quarantine service.	Enabling and Configuring Spam Quarantine, on page 268
Step 2	On the Security Management appliance, specify the Email Security appliances to include in the centralized spam quarantine.	Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance , on page 272
Step 3	Set up the Security Management appliance for sending notifications and released spam.	Configuring an Outbound IP Interface on the Security Management Appliance , on page 272
Step 4	On the Security Management appliance, configure the spam quarantine browser interface.	Configuring the IP Interface for Browser Access to the Spam Quarantine , on page 273
Step 5	Ensure that the Email Security appliance is configured to send mail to the spam quarantine.	For more information about configuring anti-spam and mail policies, see the “Anti-Spam” section of the <i>User Guide for AsyncOS for Email Security Appliances</i> .
Step 6	On the Email Security appliances, enable and configure the external spam quarantine.	For more information, see <i>User Guide for AsyncOS for Email Security Appliances</i> .
Step 7	On the Email Security appliances, disable the local quarantine.	For information about disabling the local spam quarantine to activate the external spam quarantine, see <i>User Guide for AsyncOS for Email Security Appliances</i> .

Enabling and Configuring Spam Quarantine

- [Enabling and Configuring the Spam Quarantine on the Legacy Web Interface , on page 268](#)
- [Enabling and Configuring Spam Quarantine on the New Web Interface](#)

Enabling and Configuring the Spam Quarantine on the Legacy Web Interface

-
- Step 1** Select **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 2** If you are enabling the spam quarantine for the first time after running the System Setup Wizard:
- Click **Enable**.
 - Review the end user license agreement, then click **Accept**.
- Step 3** If you are editing spam quarantine settings, click **Edit Settings**.

Step 4 Specify options:

Option	Description
Quarantine IP Interface Quarantine Port	<p>By default, the spam 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.</p> <p>If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.</p>
Deliver Messages Via	<p>All outgoing quarantine-related email (such as spam notifications and messages released from the spam quarantine) must be delivered via another appliance or server that is configured to send messages.</p> <p>You can route these messages through an SMTP or groupware server, or you can specify the outbound listener interface of an appliance (typically the Data 2 interface).</p> <p>The alternate address is used for load balancing and failover.</p> <p>If you have multiple appliances, you can use the outbound listener interface of any managed appliances for the primary and alternate addresses. Both must use the same interface (either Data 1 or Data 2) as the outbound listener.</p> <p>Read instructions on the screen for additional caveats about these addresses.</p>
Schedule Delete After	<p>Specify the number of days to hold messages before deleting them.</p> <p>Cisco recommends that you configure the quarantine to delete older messages to prevent the quarantine from filling to capacity, but you can elect not to schedule automatic deletion.</p>
Notify Cisco Upon Message Release	<p>Check the Send a copy of released messages to Cisco for analysis(recommended) checkbox if you wish to notify Cisco upon message release.</p>

Option	Description
Spam Quarantine Appearance	<p>Logo</p> <p>By default, the Cisco logo is displayed at the top of the spam quarantine page when the user logs in to view quarantined messages.</p> <p>You can view the logo on both new and legacy web interface.</p> <p>To use a custom logo instead, upload the logo. The logo should be a .jpg, .gif, or .png file that is at most 50 pixels high by 500 pixels wide.</p> <p>Login page message</p> <p>(Optional) Specify a login page message. This message is shown to end users and administrators when they log in to view the quarantine.</p> <p>If you do not specify a message, the following message appears:</p> <p>Enter your login information below. If you are unsure what to enter, please contact your administrator.</p>
Administrative Users	See Configuring Administrative User Access to the Spam Quarantine , on page 274.

Step 5 Submit and commit your changes.

What to do next

- Return to [Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance](#) , on page 272

Enabling and Configuring Spam Quarantine on the New Web Interface

Step 1 On the Security Management Appliance, click **Service Status** and hover over the  corresponding to **Spam Quarantine**, click **Edit Spam Quarantine Settings**.

Step 2 If you are using configuring spam quarantine for the first time after running the System Setup Wizard, review and accept the license agreement and click **Proceed**.

Step 3 Click the toggle switch to enable Spam Quarantine.

Step 4 Specify options:

Option	Description
Quarantine IP Interface Quarantine Port	<p>By default, the spam 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.</p> <p>If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.</p>

Option	Description
Deliver Messages Via	<p>All outgoing quarantine-related email (such as spam notifications and messages released from the spam quarantine) must be delivered via another appliance or server that is configured to send messages.</p> <p>You can route these messages through an SMTP or groupware server, or you can specify the outbound listener interface of an Email Security appliance (typically the Data 2 interface).</p> <p>The alternate address is used for load balancing and failover.</p> <p>If you have multiple Email Security appliances, you can use the outbound listener interface of any managed Email Security appliances for the primary and alternate addresses. Both must use the same interface (either Data 1 or Data 2) as the outbound listener.</p> <p>Read instructions on the screen for additional caveats about these addresses.</p>
Schedule Delete After	<p>Specify the number of days to hold messages before deleting them.</p> <p>Cisco recommends that you configure the quarantine to delete older messages to prevent the quarantine from filling to capacity, but you can elect not to schedule automatic deletion.</p>
Notify Cisco Upon Message Release	<p>You can choose to send a copy of released messages to Cisco for analysis by checking the respective box.</p>
Spam Quarantine Appearance	<p>Logo</p> <p>By default, the Cisco logo is displayed at the top of the spam quarantine page when the user logs in to view quarantined messages.</p> <p>You can view the logo on both new and legacy web interface.</p> <p>To use a custom logo instead, upload the logo. The logo should be a .jpg, .gif, or .png file that is at most 50 pixels high by 500 pixels wide.</p> <p>Login page message</p> <p>(Optional) Specify a login page message. This message is shown to end users and administrators when they log in to view the quarantine.</p> <p>If you do not specify a message, the following message appears:</p> <p>Enter your login information below. If you are unsure what to enter, please contact your administrator.</p>
Administrative Users	<p>See Configuring Administrative User Access to the Spam Quarantine , on page 274.</p>


Step 5 Click **Save**.

What to do next

- Return to [Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance](#), on page 272

Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance

The steps that you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** If you have already added the Email Security appliance to the list on this page:
- Click the name of the Email Security appliance.
 - Select the **Spam Quarantine** service.
- Step 4** If you have not yet added Email Security appliances:
- Click Add Email Appliance.
 - In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the 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**.
- The Spam Quarantine service is pre-selected.
 - Click **Establish Connection**.
 - Enter the username and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.
- 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.
- Wait for the success message to appear above the table on the page.
 - Click **Test Connection**.
 - Read the test results above the table.
- Step 5** Submit and commit your changes.
- Step 6** Repeat this procedure for each Email Security appliance for which you want to enable the spam quarantine.
-

Configuring an Outbound IP Interface on the Security Management Appliance


Configure an interface on the Security Management appliance to send quarantine-related messages (including notifications and released email) to the Email Security appliance for delivery.

Before you begin

Obtain or identify an IP address to use for the outbound interface. This will typically be the Data 2 interface on the Security Management appliance. For more information about network requirements, see [Assigning Network and IP Addresses, on page 617](#)




Note Use this procedure in conjunction with the information in [Configuring IP Interfaces, on page 610](#).

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Network IP Interfaces**.
- Step 3** Click **Add IP Interface**.
- Step 4** Enter the following settings:
- Name
 - Ethernet Port
- Typically, this will be Data 2. Specifically, this must match the data interface on the Email Security appliance that you specified for the **Primary Server** in the **Deliver Messages Via** section of the Spam Quarantine Settings page under **Management Appliance > Centralized Services > Spam Quarantine**.
- IP Address
- IP address of the interface that you just specified.
- Netmask
 - Hostname
- For example, if this is the Data 2 interface, use data2.sma.example.com .
- Do not enter information in the Spam Quarantine section for this interface.
- Step 5** Submit and commit your changes.

Configuring the IP Interface for Browser Access to the Spam Quarantine

When administrators and end users access the spam quarantine, a separate browser window opens.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Network > IP Interfaces**.
- Step 3** Click the name of the **Management** interface.
- Step 4** In the Spam Quarantine section, configure settings for access to the spam quarantine:
- By default, HTTP uses port 82 and HTTPS uses port 83.
 - Specify the URL that appears in notifications and in the spam quarantine browser window.

If you do not want to expose the hostname of your Security Management appliance to end users, you can specify an alternate hostname.

Step 5 Submit and commit your changes.

What to do next

Ensure that your DNS server can resolve the hostname that you specified for spam quarantine access.

Configuring Administrative User Access to the Spam Quarantine

All users with administrator privileges can change spam quarantine settings and view and manage messages in the spam quarantine. You do not need to configure spam quarantine access for administrator users.

If you configure access to the spam quarantine for users with the following roles, they can view, release, and delete messages in the spam quarantine:

- Email administrator
- Operator
- Read-only operator
- Help desk user
- Guest
- Custom user roles that have spam quarantine privileges

These users cannot access spam quarantine settings.

Before you begin

Create users or custom user roles that have access to the spam quarantine. For more information, see information about [Access to Quarantines for Custom User Role](#), on page 408 in [Distributing Administrative Tasks](#), on page 403

Step 1 On the Security Management appliance, click **Service Status** and hover over the  corresponding to **Spam Quarantine** and click **Edit Spam Quarantine Settings**.

Step 2 Click the toggle switch to enable Spam Quarantine.

Step 3 Click the link for the type of user to add: local, externally authenticated, or custom role.

If you have already added users or roles, click a username or role to view all eligible users or roles.

Step 4 Select the users or roles that you want to add.

Users with Administrator privileges, including Email Administrators, are not listed because they automatically have full access to the spam quarantine.

Step 5 Click **OK**.

Step 6 Click **Submit**.

What to do next**Related Topics**

[Configuring End-User Access to the Spam Quarantine](#) , on page 290

Spam Quarantine Threshold Alert

You can configure to receive alert notification(s) after you set the maximum number of spam messages that can be triggered in a duration. In addition to configuring your own alerts, you can configure Cisco Secure Email and Web Manager to generate alerts either on an hourly or on a daily basis. However, you may also set the maximum number of alerts that can be received within the time duration once the threshold is crossed.

When administrators are mapped to this custom role, they can view the quarantine mails but cannot perform a release, delete, or any other operation.

Cisco Secure Email and Web Manager ensures that you receive the alerts you set as both an email and a syslog addition.

Configuring Spam Quarantine Threshold Alert Settings Using CLI

To configure spam quarantine threshold alerts, use the **spamquarantinethresholdalert** command.

Once you execute the command, you must enable the services you avail.

You must provide values for the:

- **Threshold- Numeric Only.** Configures threshold of new quarantined spam mails for which alerts will be sent in selected time. Values range between 1-1,00,000.
- **Time Duration-** Configures the duration in hours in which the spam messages are monitored. Values range between 1800 to 86400 seconds.
- **Alert Limit-Numeric Only.**Configures the alert limit. Value ranges from 1-20.

Procedure

	Command or Action	Purpose
Step 1	spamquarantinethresholdalert Example: spamquarantinethresholdalert	Configures the spam quarantine threshold alert.

Example

Configuring Spam Quarantine Threshold Alert Settings Using GUI

Step 1 Click **Centralized Services > SPAM Quarantine**

The SPAM Quarantine page is displayed.

Step 2 Enable **Threshold Alert** checkbox.

Spam Quarantine Threshold Alerts are also governed by the System Alerts settings. To configure recipients, you must navigate to **System Administration > Alerts**.

To receive these alerts, you must subscribe to system critical alerts.

- Step 3** Enter the threshold value.
- Step 4** Choose the **Time Duration** from the drop-down.
Value ranges between half-an-hour to 24 hours.
- Step 5** Enter the **Alert Limit**.
Value ranges between 1 to 20.
- Step 6** Click **Submit**.
-

Limiting Which Recipients Have Mail Quarantined

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

Spam Quarantine Language

Each user selects a language in the spam quarantine from the Options menu at the top right of the window.

Edit Spam Quarantine Page

- [Enabling and Configuring the Spam Quarantine on the Legacy Web Interface](#) , on page 268
- [Local Versus External Spam Quarantine](#) , on page 267
- [Configuring End-User Access to the Spam Quarantine](#) , on page 290
- [Notifying End Users About Quarantined Messages](#) , on page 292

Using Safelists and Blocklists to Control Email Delivery Based on Sender

Administrators and end users can use safelists and blocklists to help determine which messages are spam. Safelists specify senders and domains that are never treated as spam. Blocklists specify senders and domains that are always treated as spam.

You can allow end users (email users) to manage the safelist and blocklist for their own email accounts. For example, an end user may receive email from a mailing list that no longer interests him. He may decide to add this sender to his blocklist to prevent emails from the mailing list from being sent to his inbox. On the other hand, end users may find that emails from specific senders are sent to their spam quarantine when they do not want them to be treated as spam. To ensure that messages from these senders are not quarantined, they may want to add the senders to their safelists.

Changes that end users and administrators make are visible to and can be changed by either.

Related Topics

- [Message Processing of Safelists and Blocklists](#) , on page 277
- [Enabling Safelists and Blocklists on the Legacy Web Interface](#), on page 278
- [External Spam Quarantine and Safelist/Blocklists](#) , on page 279
- [Adding Senders and Domains to Safelists and Blocklists \(Administrators\)](#) , on page 279
- [About End-User Access to Safelists and Blocklists](#) , on page 284
- [Backing Up and Restoring the Safelist/Blocklist](#) , on page 285
- [Troubleshooting Safelists and Blocklists](#), on page 286

Message Processing of Safelists and Blocklists

A sender's being on a safelist or blocklist does not prevent the appliance from scanning a message for viruses or determining if the message meets the criteria for a content-related mail policy. Even if the sender of a message is on the recipient's safelist, the message may not be delivered to the end user depending on other scanning settings and results.

When you enable safelists and blocklists, the appliance scans the messages against the safelist/blocklist database immediately before anti-spam scanning. If the appliance detects a sender or domain that matches a safelist or blocklist entry, the message will be splintered if there are multiple recipients (and the recipients have different safelist/blocklist settings). For example, a message is sent to both recipient A and recipient B. Recipient A has safelisted the sender, whereas recipient B does not have an entry for the sender in 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 skips anti-spam scanning, whereas the message bound for recipient B is scanned by the anti-spam scanning engine. Both messages then continue along the pipeline (through anti-virus scanning, content policies, and so on) and are subject to any configured settings.

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

Because safelists and blocklists are maintained in the spam quarantine, delivery behavior is also contingent on other anti-spam settings. For example, if you configure the "Accept" mail flow policy in the Host Access Table (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 mail flow policy that skips anti-spam scanning for certain message recipients, these recipients will not have their safelist and blocklist settings applied.

Related Topics

- [Enabling Safelists and Blocklists on the Legacy Web Interface](#), on page 278
- [External Spam Quarantine and Safelist/Blocklists](#) , on page 279

Enabling Safelists and Blocklists

- [Enabling Safelists and Blocklists on the Legacy Web Interface](#), on page 278
- [Enabling Safelists and Blocklists on the New Web Interface](#)

Enabling Safelists and Blocklists on the Legacy Web Interface

Before you begin

- The spam quarantine must be enabled. See [Setting Up the Centralized Spam Quarantine](#) , on page 268.

Step 1 Navigate to **Management Appliance > Centralized Services > Spam Quarantine**.

Step 2 Under **End-User Safelist/Blocklist**, click **Edit Settings**.

Step 3 Select **Enable End User Safelist/Blocklist Feature**.

Step 4 Specify **Maximum List Items Per User**.

This is the maximum number of addresses or domains for each list, for each recipient. If you allow a large number of list entries per user, system performance might be adversely affected.

Step 5 Select **Update Frequency**.

This value determines how often AsyncOS updates the safelists/blocklists on the appliances that use the external spam quarantine. The significance of this setting is described in [External Spam Quarantine and Safelist/Blocklists](#) , on page 279.

Step 6 Submit and commit your changes.

Enabling Safelists and Blocklists on the New Web Interface

Before you begin

- The spam quarantine must be enabled. See [Setting Up the Centralized Spam Quarantine](#) , on page 268.

Step 1 On the Security Management appliance, click **Service Status** and hover over the  icon corresponding to **Spam Quarantine**.

Step 2 Click **Edit Safelist/Blocklist Settings**.

Step 3 Click the toggle switch to enable Safelist/Blocklist Settings.

Step 4 Specify the **Maximum List Items Per User**.

This is the maximum number of addresses or domains for each list, for each recipient. If you allow a large number of list entries per user, system performance might be adversely affected.

Step 5 Select **Update Frequency**.

This value determines how often AsyncOS updates the safelists/blocklists on the Email Security appliances that use the external spam quarantine. The significance of this setting is described in [External Spam Quarantine and Safelist/Blocklists](#) , on page 279.

Step 6 Click **Submit**.

External Spam Quarantine and Safelist/Blocklists

Because the appliance evaluates senders in safelists and blocklists when processing incoming mail, safelists and blocklists that are stored on a Security Management appliance must be sent to the appliance in order to be applied to incoming mail. When you configure the safelist/blocklist feature on a Security Management appliance, you configure the frequency of these updates.

Adding Senders and Domains to Safelists and Blocklists (Administrators)

Manage safelists and blocklists via the spam quarantine interface.

You can also see whether many recipients (end users in your organization) have included a particular sender or domain in allowed list or blocked list.

Administrators see and work with the superset of the same entries that each end user sees and works with.

Before you begin

- Ensure that you can access the spam quarantine. See [Accessing the Spam Quarantine \(Administrative Users\)](#), on page 299.
- Enable access to the safelist/blocklist. See [Enabling Safelists and Blocklists on the Legacy Web Interface](#), on page 278.
- (Optional) To import safelist/blocklists instead of building these lists using the procedure in this section, use the process described in [Backing Up and Restoring the Safelist/Blocklist](#), on page 285.
- Understand the required format of safelist and blocklist entries. See [Syntax for Safelists and Blocklist Entries](#), on page 283.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click **Quarantine > Spam Quarantine > Search**.
Or
Choose **Email > Message Quarantine > Spam Quarantine** and select the **Options** drop-down menu in the upper right corner of the page.
- Step 2** Choose **Safelist** or **Blocklist**.
- Step 3** (Optional) Search for a sender or recipient.
- Step 4** Do one or more of the following:

To	Do This
Add multiple senders for a recipient	<p>To add multiple senders for a recipient on the new web interface:</p> <ol style="list-style-type: none"> a. Select Recipient tab. b. Click on the + icon to add a recipient address and sender list. c. Enter the recipient email address. d. Enter the sender email addresses and domains. Put each entry on a separate line, or separate each entry with a comma. e. Click <input checked="" type="checkbox"/> to save the entry. <p>To modify an existing sender address, select the checkbox next to the required recipient address, click the edit icon, modify the sender address and click <input checked="" type="checkbox"/> to save the entry.</p> <p>To add multiple senders for a recipient on the legacy web interface:</p> <ol style="list-style-type: none"> a. Select View by: Recipient b. Click Add, or click Edit for a recipient. c. Enter or edit the recipient email address. d. Enter sender email addresses and domains. Put each entry on a separate line, or separate each entry with a comma. e. Click Submit.

To	Do This
Add multiple recipients for a sender	<p>To add multiple recipient for a sender on the new web interface:</p> <ol style="list-style-type: none"> Select Sender tab. Click + to add a sender address and recipient list. Enter the sender address or domain. Enter the recipient email addresses. Put each entry on a separate line, or separate each entry with a comma. Click <input checked="" type="checkbox"/> to save the entry. <p>To modify an existing recipient address, select the checkbox next to the required sender address, click the edit icon, modify the sender address and click <input checked="" type="checkbox"/> to save the entry.</p> <p>To add multiple recipient for a sender on the legacy web interface:</p> <ol style="list-style-type: none"> Select View by: Sender Click Add, or click Edit for a sender. Enter or edit the sender address or domain. Enter recipient email addresses. Put each entry on a separate line, or separate each entry with a comma. Click Submit.
Delete all senders associated with a recipient	<p>To delete all senders associated with a recipient on the new web interface:</p> <ol style="list-style-type: none"> Select the checkbox next to the recipient or sender address to select the entry. You can select and delete all entries. Click on the trash can icon to delete an entire table row. <p>To delete all senders associated with a recipient on the legacy web interface:</p> <ol style="list-style-type: none"> Select a View by option. Click a trash can icon to delete an entire table row.

To	Do This
Delete all recipients associated with a sender	<p>To delete all recipients associated with a sender on the new web interface:</p> <ol style="list-style-type: none"> a. Select the checkbox next to the recipient or sender address to select the entry. You can select and delete all entries. b. Click on the trash can icon to delete an entire table row. <p>To delete all recipients associated with a sender on the legacy web interface:</p> <ol style="list-style-type: none"> a. Select a View by option. b. Click a trash can icon to delete an entire table row.
Delete individual senders for a recipient	<p>To delete individual senders for a recipient on the new web interface:</p> <ol style="list-style-type: none"> a. Select the checkbox next to the recipient or sender address to select the entry. You can select and delete multiple entries. b. Click on the edit icon to modify an individual recipient or sender. c. Add or remove entries from the text box. You must leave at least one entry. d. Click <input checked="" type="checkbox"/> to save the entry. <p>To delete individual senders for a recipient on the legacy web interface:</p> <ol style="list-style-type: none"> a. Select a View by option. b. Click Edit for an individual recipient or sender. c. Add or remove entries from the text box. You must leave at least one entry. d. Click Submit.

To	Do This
Delete individual recipients for a sender	<p>To delete individual recipient for a sender on the new web interface:</p> <ol style="list-style-type: none"> Select the checkbox next to the recipient or sender address to select the entry. You can select and delete multiple entries. Click on the edit icon to modify an individual recipient or sender. Add or remove entries from the text box. You must leave at least one entry. Click <input checked="" type="checkbox"/> to save the entry. <p>To delete individual senders for a recipient on the legacy web interface:</p> <ol style="list-style-type: none"> Select a View by option. Click Edit for an individual recipient or sender. Add or remove entries from the text box. You must leave at least one entry. Click Submit.

What to do next

Related Topics

- [Syntax for Safelists and Blocklist Entries](#) , on page 283
- [Clearing All Safelists and Blocklists](#) , on page 284

Syntax for Safelists and Blocklist Entries

Senders can be added to safelists and blocklists using the following formats:

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

An identical entry, such as a sender address or a domain, cannot be included on both the safelist and the blocklist at the same time. However, a domain can be on a safelist while an email address for a sender belonging to that domain is on the blocklist (or vice versa), and both rules apply. For example, if *example.com* is on the safelist, *george@example.com* can be on the blocklist. In this case, the appliance delivers all mail from *example.com* without scanning for spam, except mail from *george@example.com*, which is treated as spam.

It is not possible allow or block a range of subdomains using the following syntax: *.domain.com* . However, it is possible to block a specific domain using the following syntax: *server.domain.com* .

Clearing All Safelists and Blocklists

If you need to delete all safelist and blocklist entries, including all senders and all recipients, import a file with no entries using the procedure in [Backing Up and Restoring the Safelist/Blocklist](#) , on page 285.

About End-User Access to Safelists and Blocklists

End users access their safelist and blocklist via the spam quarantine. To configure end-user access to the spam quarantine, see [Setting Up End-User Access to the Spam Quarantine via Web Browser](#) .

You may want to give your end users the URL of the spam quarantine and the instructions below, as applicable.

Related Topics

- [Adding Entries to Safelists \(End Users\)](#)
- [Adding Senders to Blocklists \(End Users\)](#)

Adding Entries to Safelists (End Users)



Note Delivery of messages from safelisted senders depends on other settings that are configured in the system. See [Message Processing of Safelists and Blocklists](#) , on page 277.

End users can add senders to safelists in two ways:

- [Adding the Sender of a Quarantined Message to the Safelist](#) , on page 284
- [Adding Senders to the Safelist Without a Quarantined Message](#) , on page 284

Adding the Sender of a Quarantined Message to the Safelist

End users can add senders to the safelist if the message has been sent to the spam quarantine.

[New Web Interface Only] Click **Release and Add to Safelist** icon to release the message and add it to the safelist.


Or

Select **Release and Add to Safelist** from the drop-down menu.

The envelope sender and the from header for the specified mail are both added to the safelist, and the released messages proceed directly to the destination queue, skipping any further work queue processing in the email pipeline.

Adding Senders to the Safelist Without a Quarantined Message

Step 1 [New Web Interface Only] Choose **Safelist**.


- Step 2** [New Web Interface Only] Enter the email address or domain. You can enter multiple domains and email addresses, separated by commas.
- Step 3** [New Web Interface Only] Click  to save the entry.
- Step 4** Access Spam Quarantine page.
- Choose **Monitor > Spam Quarantine**.
 - Select the **Options** drop-down menu in the upper right corner of the page
 - Choose **Safelist**.
 - From the Safelist dialog box, enter the email address or domain. You can enter multiple domains and email addresses, separated by commas.
 - Click **Add to List**.

Adding Senders to Blocklists (End Users)

Messages from blocklisted senders may be rejected or quarantined, depending on the safelist/blocklist action settings defined by your administrator.



Note You can add blocklist entries only using this procedure.

- Step 1** [New Web Interface Only] Choose **Blocklist**, click the + icon and enter the domain or email address that you want to blocklist. You can enter multiple domains and email addresses, separated by commas.
- Step 2** [New Web Interface Only] Click  to save the entry.
- Step 3** Access Spam Quarantine page.
- Choose **Monitor > Spam Quarantine**.
 - Choose **Blocklist** from the **Options** drop-down menu in the upper right corner of the page.
 - Enter the domain or email address that you want to blocklist. You can enter multiple domains and email addresses, separated by commas.
 - Click **Add to List**.

Backing Up and Restoring the Safelist/Blocklist

Before you upgrade your appliance or run the installation wizard, you should back up the safelist/blocklist database. Safelist/blocklist information is not included in the main XML configuration file that contains your appliance configuration settings.

Safelist/blocklist entries can also be backed up along with other data on the Security Management appliance. See [Backing Up Security Management Appliance Data](#), on page 476.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Select **Management Appliance > System Administration > Configuration File**.

Step 3 Scroll to the **End-User Safelist/Blocklist Database (Spam Quarantine)** section.

To	Do This
Export the safelist/blocklist	<p>Note the path and filename of the .csv file, and modify as needed.</p> <p>Click Backup Now.</p> <p>The appliance saves a .csv file to the /configuration directory of the appliance using the following naming convention:</p> <p><i>slbl<serial number><timestamp>.csv</i></p>
Import the safelist/blocklist	<p>Caution This process will overwrite all existing entries in safelists and blocklists for all users.</p> <p>Click Select File to Restore.</p> <p>Select the desired file from the list of files in your configuration directory.</p> <p>Select the safelist/blocklist backup file that you want to restore.</p> <p>Click Restore.</p>

Troubleshooting Safelists and Blocklists

To troubleshoot issues with safelists and blocklists, you can view the log files or system alerts.

When an email is blocked due to safelist/blocklist settings, the action is logged in the ISQ_log files or the antispam log files. Emails that are safelisted are marked as safelisted with an *X-SLBL-Result-Safelist* header. Emails that are blocklisted are marked as blocklisted with an *X-SLBL-Result-Blocklist* header.

Alerts are sent out when the database is created or updated, or if there are errors in modifying the database or running the safelist/blocklist processes.

For more information about alerts, see [Managing Alerts, on page 499](#).

For more information about log files, see [Logging, on page 565](#).

Related Topics

- [Message from Safelisted Sender Was Not Delivered](#), on page 286

Message from Safelisted Sender Was Not Delivered

Problem

Message from a safelisted sender was not delivered.

Solution

Possible causes:

- The message was dropped for malware or content violations. See [Message Processing of Safelists and Blocklists](#), on page 277.

- If you have multiple appliances and the sender was recently added to the safelist, then safelist/blocklists might not have been synchronized at the time the message was processed. See [External Spam Quarantine and Safelist/Blocklists](#) , on page 279 .

Configuring Spam Management Features for End Users

To	See
Understand the benefits and limitations of the different authentication methods for end-user access to spam management features.	Configuring End-User Access to the Spam Quarantine , on page 290 and subsections
Allow end users to access the spam quarantine directly via browser.	Authentication Options for End Users Accessing Spam Management Features , on page 287
Send users a notification when messages addressed to them are routed to the spam quarantine. Notifications can include links for access to the spam quarantine.	Notifying End Users About Quarantined Messages , on page 292
Allow users to specify email addresses and domains of senders whom they know to be safe, and of senders whom they know to be sending spam or other unwanted mail.	Using Safelists and Blocklists to Control Email Delivery Based on Sender , on page 276

Related Topics

- [Authentication Options for End Users Accessing Spam Management Features](#) , on page 287
- [Setting Up End-User Access to the Spam Quarantine via Web Browser](#) , on page 289
- [Notifying End Users About Quarantined Messages](#) , on page 292
- [Configuring End-User Quarantine for Shared Mailbox](#) , on page 296

Authentication Options for End Users Accessing Spam Management Features



Note Mailbox authentication does not allow users to view messages addressed to an email alias.

For End-User Spam Quarantine Access	Do This
Directly via web browser, authentication required and Via a link in a notification, authentication required	<ol style="list-style-type: none"> 1. In the End User Quarantine Access settings, choose LDAP, SAML 2.0, or Mailbox (IMAP/POP). 2. In the Spam Notifications settings, deselect Enable login without credentials for quarantine access.

For End-User Spam Quarantine Access	Do This
Directly via web browser, authentication required and Via a link in a notification, authentication not required	<ol style="list-style-type: none"> 1. In the End User Quarantine Access settings, choose LDAP, SAML 2.0, or Mailbox (IMAP/POP). 2. In the Spam Notifications settings, select Enable login without credentials for quarantine access.
Only via a link in a notification, authentication not required	In the End User Quarantine Access settings, choose None as the authentication method.
No access	In the End User Quarantine Access settings, deselect Enable End-User Quarantine Access .

Related Topics

- [LDAP Authentication Process](#) , on page 288
- [IMAP/POP Authentication Process](#) , on page 289
- [SAML 2.0 Authentication Process](#), on page 289
- [Configuring End-User Access to the Spam Quarantine](#) , on page 290
- [Notifying End Users About Quarantined Messages](#) , on page 292
- [Configuring LDAP to Work with the Spam Quarantine](#), on page 371
- [About End-User Access to Safelists and Blocklists](#) , on page 284

LDAP Authentication Process

1. A user enters his or her username and passphrase into the web UI login page.
2. The spam quarantine connects to the specified LDAP server either to perform an anonymous search or as an authenticated user with the specified “Server Login” DN and passphrase. For Active Directory, you will usually need to have the server connect on the “Global Catalog port” (it is in the 6000s) and you need to create a low privilege LDAP user that the spam quarantine can bind as in order to execute the search.
3. The spam quarantine then searches for the user using the specified BaseDN and Query String. When a user’s LDAP record is found, the spam quarantine then extracts the DN for that record and attempts bind to the directory using the user records’ DN and the passphrase they entered originally. If this passphrase check succeeds then the user is properly authenticated, but the spam quarantine still needs to determine which mailboxes’ contents to show for that user.
4. Messages are stored in the spam quarantine using the recipient's envelope address. After a user's passphrase is validated against LDAP, the spam quarantine then retrieves the “Primary Email Attribute” from the LDAP record to determine which envelope address they should show quarantined messages for. The “Primary Email Attribute” can contain multiple email addresses which are then used to determine what envelope addresses should be displayed from the quarantine for the authenticated user.

Related Topics

- [Authentication Options for End Users Accessing Spam Management Features](#) , on page 287
- [Integrating With LDAP](#), on page 371

IMAP/POP Authentication Process

1. Depending on your mail server configuration, a user enters their username (joe) or email address (joe@example.com) and passphrase into the web UI login page. You can modify the Login Page Message to tell your users whether they should enter a full email address or just their username (see [Configuring End-User Access to the Spam Quarantine , on page 290](#)).
2. The spam quarantine connects to the IMAP or POP server and uses the entered login (either username or email address) and passphrase to try to log into the IMAP/POP server. If the passphrase is accepted then the user is considered authenticated and the spam quarantine immediately logs out of the IMAP/POP server.
3. Once the user is authenticated, the spam quarantine lists email for the user, based on the email address:
 - If you have configured the spam quarantine to specify a domain to append to bare usernames (like joe), then this domain is appended and that fully qualified email address is used to search for matching envelopes in the quarantine.
 - Otherwise, the spam quarantine uses the entered email address to search for matching envelopes.

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

<http://www.washington.edu/imap/>

SAML 2.0 Authentication Process

See section *SSO Using SAML 2.0* in the *Cisco Content Security Management Appliance Guide*

Setting Up End-User Access to the Spam Quarantine via Web Browser

-
- Step 1** Understand the benefits and limitations of the different authentication methods for end-user access to spam management features.
- Step 2** If you will authenticate end users using LDAP, configure an LDAP server profile, including the **Spam Quarantine End-User Authentication Query** settings on the **System Administration > LDAP > LDAP Server Profile** page.
- Example:**
- If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the **System Administration > SAML** page.
- [Integrating With LDAP, on page 371](#) and subsections
- [SSO Using SAML 2.0, on page 525](#)
- Step 3** Configure end-user access to the spam quarantine.
- [Configuring End-User Access to the Spam Quarantine , on page 290](#)
- Step 4** Determine the URL for end-user access to the spam quarantine.
- [Determining the URL for End-User Access to the Spam Quarantine, on page 291](#)
-

What to do next

Related Topics


- [Configuring End-User Access to the Spam Quarantine](#) , on page 290
- [Determining the URL for End-User Access to the Spam Quarantine](#), on page 291
- [Which Messages an End User Sees](#) , on page 291

Configuring End-User Access to the Spam Quarantine

Administrative users can access the spam quarantine whether or not end-user access is enabled.

Before you begin

See requirements in [Authentication Options for End Users Accessing Spam Management Features](#) , on page 287.

- Step 1** If you are on the legacy interface, navigate to **Management Appliance > Centralized Services > Monitor > Spam Quarantine > Edit Settings**, and then scroll down to **End-User Quarantine Access**. If you are on the new web interface, then navigate to Security Management appliance , click **Service Status** and hover on  icon and click **Edit End-User Quarantine Settings**. You will be redirected to the legacy interface.
- Step 2** Select **Enable End-User Quarantine Access**.
- Step 3** Specify the method to use to authenticate end users when they attempt to view their quarantined messages.

Select This Option	More Information
None	Choose this option to make the quarantined messages accessible to the end-users via links in the spam notification without additional authentication.
Mailbox (IMAP/POP)	<p>For sites without an LDAP directory to use for authentication, the quarantine can validate user email addresses and passphrases against a standards-based IMAP or POP server that holds their mailbox.</p> <p>When logging in to the spam quarantine, end users enter their full email address and mailbox passphrase.</p> <p>If the POP server advertises APOP support in the banner, then for security reasons (i.e., to avoid sending the passphrase in the clear) the Cisco appliance will only use APOP. If APOP is not supported for some or all users then the POP server should be reconfigured to not advertise APOP.</p> <p>Select SSL if you have configured your server to use it. If users enter username only, you can specify a domain to add to automatically complete the email address. Enter the domain of the envelope for users logging in to “Append Domain to Unqualified Usernames.”</p>
LDAP	Configure LDAP settings as described in the sections referenced in the Before You Begin section of this topic.
SAML 2.0	<p>Enable single sign-on for Spam Quarantine.</p> <p>Before using this option, make sure that you have configured all the settings on Management Appliance > System Administration > SAML page. See section <i>SSO Using SAML 2.0</i> in the <i>Cisco Content Security Management Appliance Guide</i>.</p>

Step 4 Specify whether or not to display message bodies before messages are released.

If this box is selected, users may not view the message body via the spam quarantine page. Instead, to view the body of a quarantined message, users must release the message and view it in their mail application (such as 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 5 Submit and commit your changes.

What to do next

(Optional) Customize the page that users see when they access the spam quarantine, if you have not yet done so. See setting descriptions in [Enabling and Configuring the Spam Quarantine on the Legacy Web Interface](#), on page 268.

Determining the URL for End-User Access to the Spam Quarantine

The URL that end users can use to directly access the spam quarantine is formed from the hostname of the machine and the settings (HTTP/S and port numbers) configured on the IP interface on which the quarantine has been enabled. For example, `HTTP://mail3.example.com:82`.

The end-users can now access the Spam Quarantine on the new web interface in any one of the following ways:

- When `trailblazerconfig` CLI command is enabled, use the following URL -

`https://example.com:<trailblazer-https-port>/euq-login`.

where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

- When `trailblazerconfig` CLI command is disabled, use the following URL -

`https://example.com:<https-port>/euq-login`.

where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.



Note Local and externally-authenticated users cannot log into the end-user Spam Quarantine portal.

Which Messages an End User Sees

Generally, end users see only their own messages in the spam quarantine.

Depending on the method of access (via notification or directly via web browser) and authentication method (LDAP or IMAP/POP), users may see mail for multiple email addresses in the spam quarantine.

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

If the authentication method is IMAP/POP, or the user accesses the quarantine directly via a notification, then the quarantine will display only messages for that user's email address (or the address to which the notification was sent).

For information about messages that are sent to aliases of which the user is a member, see [Recipient Email Mailing List Aliases and Spam Notifications](#) , on page 294.

Related Topics

- [Configuring End-User Access to the Spam Quarantine](#) , on page 290
- [Recipient Email Mailing List Aliases and Spam Notifications](#) , on page 294

Notifying End Users About Quarantined Messages

You can configure the system to send a notification email to some or all users when they have spam and suspected spam messages in the spam quarantine.


By default, spam notifications lists the end user's quarantined messages. Notifications include a link that you can use to view the quarantined messages in the spam quarantine. You can then decide whether to have the quarantined messages delivered to the inbox or to delete them.



Note In cluster configurations, you can choose which users receive notifications only at the machine level.

Before you begin

- For end users to manage messages listed in notifications, they must be able to access the spam quarantine. See [Configuring End-User Access to the Spam Quarantine](#) , on page 290.
- Understand and implement the authentication options for managing spam using notifications. See [Authentication Options for End Users Accessing Spam Management Features](#) , on page 287.
- If end users receive email at multiple aliases, see [Recipient Email Mailing List Aliases and Spam Notifications](#) , on page 294.

-
- Step 1** If you are on the legacy interface, navigate to **Management Appliance > Centralized Services > Spam Quarantine > Edit Settings**, and then scroll down to **Spam Notifications**. However if you are on the new web interface, navigate to Security Management appliance , click **Service Status**, hover over the  icon, and click **Edit Spam Notification Settings**. You will be redirected to the legacy interface.
- Step 2** Select **Enable Spam Notification**.
- Step 3** Enter a From: address for the notifications.
- Step 4** Specify the end-users whom you want to notify.
- Step 5** (Optional) Customize the subject for the notification.
- Step 6** (Optional) Customize the title for the notification.
- Step 7** Select the default language for notifications.
- Step 8** Configure the quarantine access for the end-users.
- a) Check the **Login without credentials** check box to automatically log users into the spam quarantine when they access it by clicking a link in a notification. The end-users can release messages by clicking the **Release** links in the notification. If you uncheck this option, the end-users cannot release messages by clicking the **Release** links in the notification.

This option is visible only if you choose one of the following end-user authentication methods: Mailbox (IMAP/POP), LDAP, or SAML 2.0. If you have chosen None as the authentication method, when the end-users click on the links in the spam notification, they are automatically logged into the spam quarantine.

- b) Set an expiration period (in days) for the links in the notification. Enter a number between 0 and 365. These links will expire automatically after the specified period. Enter 0 if you do not want the links to expire.

(For Mailbox (IMAP/POP), LDAP, and SAML 2.0) This option is configurable only if you check the **Login without credentials** check box.

You can also set the expiration period using the **spamdigestconfig** command in the CLI.

Step 9

Customize the message body:

- a) (Optional) Customize the default text and variables.

To insert a variable, place the cursor where you would like the variable inserted and then click the name of the variable in the Message Variables listing on the right. Or type in the variable.

The following message variables are expanded to the actual value for the specific end user:

- **New Message Count** (%new_message_count%)— The number of new messages since the user last logged in.
 - **Total Message Count** (%total_message_count%)— The number of messages for the user in the spam 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%)— A list of the user’s new quarantined messages, showing sender, message subject, date, and a link to release the message. The user clicks a message subject to view the message in the spam quarantine.
 - **New Message Table without Subject** (%new_quarantine_messages_no_subject%)— Similar to New Message Table, but only a “View Message” link is shown in place of the subject for each message.
- b) Choose whether to show or hide the links to view all the quarantined messages in a spam notification. Under **Show link to see all quarantined messages in Notification Mails**, choose **Yes** or **No** depending on your requirement.

(For Mailbox (IMAP/POP), LDAP, and SAML 2.0). This option is visible only if you check the **Login without credentials** check box (under Quarantine Access).

If you choose **Yes**, you can force the end-user to authenticate before accessing the spam quarantine. Check **Challenge Access**. This option is not available if you have chosen None as the end-user authentication method.

You can also show or hide the links using the **spamdigestconfig** command in the CLI.

- c) Click **Preview Message** to verify that the message is as you want it to be.

Step 10

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

Step 11

Specify the address to which bounced notifications will be sent.

Step 12

(Optional) Select **Consolidate messages sent to the same LDAP user at different addresses**.

Step 13

Set the notification schedule.

Step 14 Submit and commit your changes.

What to do next

To ensure that end users receive these notifications, consider recommending that they add the From: address for the spam quarantine notification emails to the “allowed list” in the junk mail settings of their mail application (such as Microsoft Outlook or Mozilla Thunderbird.)

Related Topics

- [Recipient Email Mailing List Aliases and Spam Notifications](#) , on page 294
- [Testing Notifications](#), on page 295
- [Troubleshooting Spam Notifications](#) , on page 295

Recipient Email Mailing List Aliases and Spam Notifications

Notifications can be sent to each Envelope Recipient that has quarantined email, including mailing lists and other aliases. Each mailing list receives a single digest. If you send notifications to a mailing list, all subscribers to the list will receive the notification. Users who belong to multiple email aliases, or who belong to LDAP groups that receive notifications, or who use several email addresses, may receive multiple spam notifications. The following table shows example situations in which users may receive multiple notifications.

Table 71: Notifications per Address/Alias

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

If you use LDAP authentication, you can choose not to send notifications to mailing list aliases. Or, if you choose to send spam notifications to mailing list aliases, you can prevent some occurrences of multiple notifications. .

Users who access the spam quarantine by clicking a link in a notification will not see quarantined messages for any other aliases that the end-user may have, unless the appliance is using a spam quarantine alias consolidation query for email notifications. If the notification was sent to a distribution list that is expanded after processing by the appliance, then multiple recipients may have access to the same quarantine for that list.

This means that all subscribers to a mailing list will receive the notification and can log in to the quarantine to release or delete messages. In this case, end users visiting the quarantine to view messages mentioned in a notification may find that those messages have already been deleted by other users.



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

Testing Notifications

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

Troubleshooting Spam Notifications

Related Topics

- [User Receives Multiple Notifications](#) , on page 295
- [Recipient Does Not Receive Notifications](#) , on page 295
- [User Receives Multiple Notifications](#) , on page 295
- [Recipient Does Not Receive Notifications](#) , on page 295

User Receives Multiple Notifications

Problem

A user receives multiple spam notifications for a single message.

Solution

Possible causes:

- The user has multiple email addresses and the spam message was sent to more than one of those addresses.
- The user is a member of one or more email aliases that received the spam message. To minimize duplications, and for more information, see [Recipient Email Mailing List Aliases and Spam Notifications](#) , on page 294.

Recipient Does Not Receive Notifications

Problem

Recipient is not receiving spam notifications.

Solution

- If notifications are being sent to the “Deliver Bounce Messages To:” address instead of to spam recipients, this means that spam notifications are enabled, but spam quarantine access is not enabled. See [Authentication Options for End Users Accessing Spam Management Features](#) , on page 287.
- Have the user check the junk mail settings of their email client.
- Check for issues with the appliance or server that you specified for **Deliver Messages Via** in [Enabling and Configuring the Spam Quarantine on the Legacy Web Interface](#) , on page 268.

Configuring End-User Quarantine for Shared Mailbox

You can now access the End-User Quarantine (EUQ) of the Shared Mailbox and perform any actions on the spam quarantined messages when an administrator enables single sign-on to access EUQ and you have delegated access to that Shared Mailbox. It reduces the workload on administrators and assists in the timely delivery of quarantined messages.

You can access EUQ to search the spam quarantine messages of the Shared Mailbox if you can log into EUQ through SAML 2.0 authentication. You can view the spam quarantined messages of your Primary Mailbox, and you can now add the Shared Mailbox to which you have access and view the spam quarantined messages of that Shared Mailbox.

EUQ allows you to add multiple Shared Mailboxes and provides an option to view, search, release, release and add to safelist, and delete the spam quarantined messages.

Related Topics

- [Accessing EUQ for Shared Mailbox](#) , on page 296

Accessing EUQ for Shared Mailbox

Before you begin:

- The administrator must register an Microsoft Azure Active Directory application to access the identity information.

For more details on registering the Microsoft Azure Active Directory application, see [Registering Azure Active Directory Application, on page 631](#).

- The administrator must provide the redirect Uniform Resource Identifier (URI) as the URI of their EUQ.
- The administrator must grant user.read permission rights in Microsoft Azure Active Directory for the application to access the identity information.
- The administrator must enable single sign-on.
- The administrator must enable the account settings for SAML server.

You can access EUQ in the following ways:


- Click **your email quarantine** or **View All Quarantined Messages** link provided in the Spam Quarantine Notification mail.
- Log in to Secure Email and Web Manager EUQ using Spam Quarantine portal.



Note If multiple users access EUQ using the same browser on the same device, you might see the Shared Mailbox of the other user. Therefore, it is advised to use a private browser though it is less likely that multiple users are using the same browser on the same device.

Configuring Account Settings

Administrators must configure account settings in Secure Email and Web Manager to enable users to view quarantined messages of Shared Mailboxes. To configure Account Settings:

-
- Step 1** [New Web Interface Only] Click  on Secure Email and Web Manager to load the legacy web interface.
- Step 2** Go to **Centralised Services > System Administration > Account Settings** page.
The **Account Settings** page is displayed. By default, the Account Settings are disabled.
- Step 3** Click **Enable** to configure the account settings.
The **Account Profile Settings** window is displayed.
- Step 4** Select **Enable Shared Mailbox Settings** and enter the details in the following fields:
- **Profile Name:** The default name of the account profile is displayed.
 - **Description:** The default description of the account profile is displayed.
 - **Client ID:** Enter the client ID.
 - **Tenant ID:** Enter the tenant ID.
 - **Client Secret:** Enter the client secret.
 - **Redirect URL:** Enter the URL to which you must be redirected.
- Step 5** Submit and commit your changes.
The **Account Profile Settings** window now displays the entered account profile details.
- Step 6** Click **Edit** to modify the details.
-

Accessing EUQ using Spam Quarantine Notification Mail

You can access EUQ using the link provided in the Spam Notification mail (with or without authentication).
To access EUQ and view the quarantined messages of the Shared Mailbox using the Spam Notification mail, perform the following steps:

- Step 1** Click **your email quarantine** or **View All Quarantined Messages** link provided in the Spam Quarantine Notification mail.
[When authentication is not required] The **Spam Quarantine** page displays the quarantined messages of the Primary Mailbox, and the Shared Mailbox is not added. You can also search for any required quarantined messages.
- Step 2** [When authentication is not required] Go to step 6 of the procedure.
- Step 3** [Applicable for authentication only] Enter your login credentials and authenticate.
The **Permission Requested** page is displayed. Note that you are prompted to grant access permission rights only for the first time you access EUQ.
- Step 4** [Applicable for authentication only] Click **Accept** to grant the access permission rights to Secure Email and Web Manager to access and view your messages.
The **Spam Quarantine** page displays the quarantined messages of the Shared Mailbox and Primary mailbox. If you do not have access to the entered Shared Mailbox, an error message is displayed, and the quarantined messages of your Primary Mailbox are displayed.

- Step 5** [Applicable for authentication only] Add a Shared Mailbox. See [Adding Shared Mailbox, on page 298](#) to add a Shared Mailbox.
- Step 6** Enter the quarantined message in the **Search Messages and another random message** text box and click **Search** to search for a particular quarantined message.
- The quarantined message that you searched is displayed in the **Search Results** window.
- Step 7** Select the quarantined message of the Shared Mailbox from the **Search Results** window and select the actions from the **Select Actions** drop-down list.
- Step 8** Click **Submit** to release or delete the quarantined messages of the Shared Mailbox.

Accessing EUQ using Spam Quarantine Portal

You can access EUQ using the Spam Quarantine portal.

To access EUQ and view the quarantined messages of the Shared Mailbox using Spam Quarantine portal, perform the following steps:

- Step 1** Log in to the Spam Quarantine portal using your credentials.
- Step 2** Log in to Secure Email and Web Manager EUQ with SAML account.
- The **Spam Quarantine** page is displayed.
- Step 3** Add a Shared Mailbox. See [Adding Shared Mailbox, on page 298](#) to add a Shared Mailbox.
- Step 4** Select the Shared Mailbox from **View Messages for Mailbox** drop-down list to see the list of quarantined messages of that Shared Mailbox.
- Step 5** Enter the quarantined message in the **Search Messages and another random message** text box and click **Search** to search for a particular quarantine message.
- The quarantined message that you searched is displayed in the **Search Results** window.
- Step 6** Select the quarantined message of the Shared Mailbox from the **Search Results** window and select the actions from the **Select Actions** drop-down list and click **Submit** to release or delete the quarantined messages of the Shared Mailbox.

Adding Shared Mailbox

You can add a Shared Mailbox to which you have access to view the quarantined messages of that Shared Mailbox.



Note The respective mailbox ID is displayed at the top right corner of the **Spam Quarantine** page, when you access the quarantine messages of your Primary Mailbox or Shared Mailbox.

To add a Shared Mailbox, perform the following steps:

- Step 1** Click the **View Message for mailbox** drop-down list and select **Add Shared mailbox** on the Spam Quarantine page.
- Step 2** Enter the name of the mailbox in **Mailbox name** and click **Add Mailbox** in the **Add Mailbox** pop-up window. Now, the Shared Mailbox is added to the **View Message for Mailbox** drop-down list.

If you do not have access to the entered Shared Mailbox, an error message is displayed.

Note that the list of added Shared Mailbox is retained in the cookie. If you are using the same browser and the cookie is available, the Shared Mailbox is retained. You have to add the Shared Mailbox again, if you log into EUQ using a different system.

Note If the administrator disables your Shared Mailbox access, but you have already added that Shared Mailbox, then you can access it for 40 minutes until the next refresh token from Microsoft Azure is received.

When the administrator enables your access to the Shared Mailbox, you cannot add the Shared Mailbox immediately, and it takes up to 30 minutes to access it.

Managing Messages in the Spam Quarantine

This section explains how to work with messages in local or external spam quarantines.

Administrative users can see and manage all messages in the spam quarantine.

Related Topics

- [Accessing the Spam Quarantine \(Administrative Users\), on page 299](#)
- [Searching for Messages in the Spam Quarantine, on page 299](#)
- [Viewing Messages in the Spam Quarantine, on page 300](#)
- [Delivering Messages in the Spam Quarantine, on page 301](#)
- [Deleting Messages from the Spam Quarantine, on page 301](#)

Accessing the Spam Quarantine (Administrative Users)

Administrative users can see and manage all messages in the spam quarantine.

Accessing the Spam Quarantine (Administrative Users)

Administrative users can see and manage all messages in the spam quarantine.

Step 1 [New Web Interface Only] On the Security Management appliance, choose **Quarantine > Spam Quarantine > Search**.

Step 2 Select **Email > Message Quarantine > Spam Quarantine**, then click the **Spam Quarantine** link.

The spam quarantine opens in a separate browser window.

Searching for Messages in the Spam Quarantine

Step 1 Specify an envelope recipient.

Note You can enter a partial address.

- Step 2** Select whether the search results should match the exact recipient you entered, or whether the results should contain, start with, or end with your entry.
- Step 3** Enter a date range to search through. Click the calendar icons to select a date.
- Step 4** Specify a From: address, and select whether the search results should contain, match exactly, start with, or end with the value you entered.
- Step 5** Click **Search**. Messages matching your search criteria are displayed below the Search section of the page.
-

What to do next

Related Topics

[Searching Very Large Message Collections, on page 300](#)

Searching Very Large Message Collections

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

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

Viewing Messages in the Spam Quarantine

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

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

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

To view additional details about the message, click the **Message Tracking** link.

Note the following:

- **Viewing Messages with Attachments**

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

In the new web interface, if a message includes an attachment, you can view the details of the attachment in the Attachments section of the message.

- **Viewing HTML Messages**

The spam quarantine attempts to render an approximation of HTML-based messages. Images are not displayed.

- **Viewing Encoded Messages**

Base64-encoded messages are decoded and then displayed.

Delivering Messages in the Spam Quarantine

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

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

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

Deleting Messages from the Spam Quarantine

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

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

To delete all messages in the spam quarantine, disable the quarantine (see [About Disabling the External Spam Quarantine](#), on page 301) and then click the **Delete All Messages** link. The number in parenthesis at the end of the link is the number of messages in the spam quarantine.

Disk Space for the Spam Quarantine

Available disk space for the quarantine varies by appliance model. See [Viewing Disk Space, Quotas and Usage](#), on page 522.

By default, messages in the spam quarantine are automatically deleted after a set amount of time. If the quarantine gets full, older spam is deleted. To change this setting, see [Enabling and Configuring the Spam Quarantine on the Legacy Web Interface](#), on page 268.

Related Topics

About Disabling the External Spam Quarantine

If you disable the spam quarantine:

- If messages are present in the spam quarantine when it is disabled, you can opt to delete all of the messages.
- Any mail policies set to quarantine spam or suspected spam will instead be set to deliver the message. You may need to adjust mail policies on the Email Security appliance.
- To completely disable an external spam quarantine, disable it on both the appliance and the Security Management appliance.

Disabling an external spam quarantine on the appliance only does not delete the external quarantine or its messages and data.

Troubleshooting Spam Quarantine Features

- [Troubleshooting Safelists and Blocklists](#), on page 286
- [Troubleshooting Spam Notifications](#) , on page 295



CHAPTER 10

Centralized Policy, Virus, and Outbreak Quarantines

This chapter contains the following sections:

- [Overview of Centralized Quarantines](#) , on page 303
- [Centralizing Policy, Virus, and Outbreak Quarantines](#) , on page 305
- [Managing Policy, Virus, and Outbreak Quarantines](#), on page 311
- [Working with Messages in Policy, Virus, or Outbreak Quarantines](#), on page 321
- [Troubleshooting Centralized Policy Quarantines](#) , on page 329

Overview of Centralized Quarantines

Messages processed by certain filters, policies, and scanning operations on an Email Security appliance can be placed into quarantines to temporarily hold them for further action. You can centralize quarantines from multiple Email Security appliances on a Cisco Content Security Management appliance.

Benefits of centralizing quarantines include the following:

- You can manage quarantined messages from multiple Email Security appliances in one location.
- Quarantined messages are stored behind the firewall instead of in the DMZ, reducing security risk.
- Centralized quarantines can be backed up as part of the standard backup functionality on the Security Management appliance.

Anti-virus scanning, Outbreak Filters, and Advanced Malware Protection (File Analysis) each have a single dedicated quarantine. You create policy quarantines to hold messages that are caught by message filtering, content filtering, and Data Loss Prevention policies.

The Policy, Virus and Outbreak Quarantines section in the legacy web interface is labeled as Other Quarantines in the new web interface. For more information, see [Viewing Messages in Quarantines](#) , on page 322.

For additional information about quarantines, see the documentation for your Email Security appliance.

Quarantine Types

Quarantine Type	Quarantine Name	Created by the System by Default?	Description	More Information
Advanced Malware Protection	File Analysis	Yes	Holds messages that are sent for file analysis, until a verdict is returned.	<ul style="list-style-type: none"> • Managing Policy, Quarantines • Working with Message Filters or Outbreak Quarantines
Virus	Virus	Yes	Holds messages that may be transmitting malware, as determined by the anti-virus engine.	
Outbreak	Outbreak	Yes	Holds messages caught by Outbreak Filters as potentially being spam or malware.	
Policy	Policy	Yes	Holds messages caught by message filters, content filters, and DLP message actions. A default Policy quarantine has been created for you.	
	Unclassified	Yes	Holds messages only if a quarantine that is specified in a message filter, content filter, or DLP message action has been deleted. You cannot assign this quarantine to any filter or message action.	
	(Policy quarantines that you create)	No	Policy quarantines that you create for use in message filters, content filters, and DLP message actions.	
Spam	Spam	Yes	Holds spam or suspected spam messages for the message's recipient or an administrator to review. The spam quarantine is not included in the group of policy, virus, and outbreak quarantines and is managed separately from all other quarantines.	Spam Quarantine, on p

Centralizing Policy, Virus, and Outbreak Quarantines

Procedure

	Command or Action	Purpose
Step 1	If your Email Security appliance is in your DMZ and your Security Management appliance is behind your firewall, open a port in the firewall to allow the appliances to exchange centralized policy, virus, and outbreak quarantine data.	Firewall Information, on page 621
Step 2	On the Security Management appliance, enable the feature.	Enabling Centralized Policy, Virus, and Outbreak Quarantines on the Security Management Appliance , on page 307
Step 3	On the Security Management appliance, allocate disk space for non-spam quarantines.	Managing Disk Space , on page 521
Step 4	<p>(Optional)</p> <ul style="list-style-type: none"> • Create centralized policy quarantines on the Security Management appliance with desired settings. • Configure settings for the centralized virus and outbreak quarantines, and for the default policy quarantines. <p>If you configure these settings before migration, you can refer to the existing settings on your Email Security appliances.</p> <p>You can also create required quarantines while configuring custom migration, or quarantines will be created for you during automatic migration. All quarantines created during migration have default settings.</p> <p>Local quarantine settings are not retained in the centralized quarantine, even if the quarantine name is the same.</p>	<ul style="list-style-type: none"> • Configuring Policy, Virus, and Outbreak Quarantines , on page 314 • Checking the Settings of System-Created Quarantines , on page 314.
Step 5	<p>On the Security Management appliance, add Email Security appliances to manage, or select the Policy, Virus and Outbreak Quarantines option from the centralized services of an already-added appliance.</p> <ul style="list-style-type: none"> • If your Email Security appliances are clustered, all appliances that belong to a particular level (machine, group, or cluster) must be added to the Security Management appliance before you enable centralized Policy, Virus and Outbreak Quarantines on any Email Security appliance in the cluster. 	Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance, on page 307

	Command or Action	Purpose
Step 6	Commit your changes.	
Step 7	On the Security Management appliance, configure migration of existing policy quarantines from Email Security appliances.	Configuring Migration of Policy, Virus, and Outbreak Quarantines , on page 308
Step 8	<p>On an Email Security appliance, enable the centralized policy, virus, and outbreak quarantines feature.</p> <ul style="list-style-type: none"> • Important If you have policy, virus, and outbreak quarantines configured on an Email Security appliance, migration of quarantines and all their messages begins as soon as you commit this change. 	<p>See the “Centralizing Services on a Cisco Content Security Management appliance” chapter in the documentation for your Email Security appliance, specifically the following sections:</p> <ul style="list-style-type: none"> • “About Migration of Policy, Virus, and Outbreak Quarantines” • “Centralizing Policy, Virus, and Outbreak Quarantines”
Step 9	<p>Migrate additional Email Security appliances.</p> <ul style="list-style-type: none"> • Only one migration process can be in progress at any time. Do not enable centralized policy, virus, and outbreak quarantines on another Email Security appliance until the previous migration is complete. 	
Step 10	<p>Edit centralized quarantine settings as needed.</p> <ul style="list-style-type: none"> • Quarantines created during migration are created with default settings, not the settings in the originating local quarantines, even if the centralized and local quarantine names are the same. 	Configuring Policy, Virus, and Outbreak Quarantines , on page 314
Step 11	<p>If message filters, content filters, and DLP message actions could not be automatically updated with the names of centralized quarantines, manually update those configurations on your Email Security appliances.</p> <ul style="list-style-type: none"> • In cluster configurations, filters and message actions can be automatically updated on a particular level only if filters and message actions are defined at that level. 	See the documentation for message filters, content filters, and DLP Message Actions in the online help or user guide for your Email Security appliance.
Step 12	(Recommended) Specify an Email Security appliance to process released messages if the originating appliance is not available.	Designating an Alternate Appliance to Process Released Messages , on page 310
Step 13	If you delegate administration to custom user roles, you may need to configure access in a certain way.	Configuring Centralized Quarantine Access for Custom User Roles

Enabling Centralized Policy, Virus, and Outbreak Quarantines on the Security Management Appliance

Before you begin

Complete any steps preceding this procedure in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#), on page 305.

Step 1 Choose **Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines**.

Step 2 Click **Enable**.

Step 3 Specify the interface and port for communication with Email Security appliances:

- Accept the default selections unless you have reason to change them.
- If your Email Security appliances are not on the same network as your Security Management appliance, then you must use the Management interface.
- Use the same port that you opened in the firewall.

Step 4 Click **Submit**.

What to do next

Return to the next step in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#), on page 305.

Enabling Centralized Policy, Virus, and Outbreak Quarantines on the New Web Interface of the Appliance

Before you begin

Complete any steps preceding this procedure in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#), on page 305.

Step 1 On the Security Management appliance, click **Service Status**, hover on the  icon corresponding to **Other Quarantine**, and click **Edit Settings**.


Step 2 Click **Enable** once you are redirected to the legacy interface.

Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance

To see an consolidated view of all quarantines on all Email Security appliances, consider adding all Email Security appliances before centralizing any quarantines.

Before you begin

Make sure you have completed all procedures to this point in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#) , on page 305.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** If you have already added the Email Security appliance to the list on this page:
- Click the name of an Email Security appliance.
 - Select the **Policy, Virus, and Outbreak Quarantines** service.
- Step 4** If you have not yet added the Email Security appliance:
- Click Add Email Appliance.
 - In the Appliance Name and IP Address text fields, enter the appliance name and the IP address for the Management interface of the appliance you are adding.

Note If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.
 - The Policy, Virus and Outbreak Quarantines service is pre-selected.
 - Click **Establish Connection**.
 - Enter the user name and passphrase for an administrator account on the appliance to be managed, and then click **Establish Connection**.

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.
 - Wait for the Success message to appear above the table on the page.
- Step 5** Click **Submit**.
- Step 6** Repeat this procedure for each Email Security appliance for which you want to enable Centralized Policy, Virus, and Outbreak Quarantines.
- For example, add the other appliances in the cluster.
- Step 7** Commit your changes.
-


What to do next

Return to the next step in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#) , on page 305.

Configuring Migration of Policy, Virus, and Outbreak Quarantines

Before you begin

- Make sure that you have completed all procedures to this point in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#) , on page 305
- For caveats and information about the migration process, see the “About Migration of Policy, Virus, and Outbreak Quarantines” section in the “Centralizing Services on a Cisco Content Security Management appliance” chapter in the documentation for your Email Security appliance.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines**.

Step 3 Click **Launch Migration Wizard**.

Step 4 Choose a migration method:

If	Choose	Additional Information
<ul style="list-style-type: none"> • You want to migrate all existing policy quarantines from all associated Email Security appliances, <li style="text-align: center;">and • Policy quarantines with the same names have identical settings on all Email Security appliances, <li style="text-align: center;">and • You want to merge all policy quarantines with the same name on all Email Security appliances into a single centralized policy quarantine having that name. 	Automatic	<p>All centralized policy quarantines that are created using this process are automatically configured with default settings, regardless of the settings in the quarantines with the same names on the Email Security appliance.</p> <p>You must update those settings after migration.</p>
<ul style="list-style-type: none"> • Policy quarantines with the same names have different settings on different Email Security appliances and you want to maintain the differences, <li style="text-align: center;">or • You want to migrate some local quarantines and delete all others, <li style="text-align: center;">or • You want to migrate local quarantines to centralized quarantines with different names <li style="text-align: center;">or • You want to merge local quarantines with different names into a single centralized quarantine. 	Custom	<p>Any centralized policy quarantines that you create during migration, instead of before migration, will be configured with the default settings for new quarantines.</p> <p>You should update those settings after migration.</p>

Step 5 Click **Next**.

Step 6 If you selected **Automatic**:

Verify that the policy quarantines to be migrated and other information on this page match your expectations.

Virus, Outbreak, and File Analysis quarantines will also be migrated.

Step 7 If you selected **Custom**:

- To select whether to show quarantines from all Email Security appliances or just one., choose an option from the **Show Quarantines from:** list.
- Select which local policy quarantines move to each centralized policy quarantine.
- Create additional centralized policy quarantines as needed. These will have default settings.
- Quarantine names are case-sensitive.
- Any quarantines remaining in the table on the left will not be migrated and will be deleted from the Email Security appliance upon migration.
- You can change the quarantine mapping by selecting a quarantine from the table on the right and clicking **Remove from Centralized Quarantine**.

Step 8 Click **Next** as needed.

Step 9 Submit and commit your changes.

What to do next

Return to the next step in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#) , on page 305.


Designating an Alternate Appliance to Process Released Messages

Normally, when a message is released from a centralized quarantine, the Security Management appliance returns it for processing to the Email Security appliance that originally sent it to the centralized quarantine.

If the Email Security appliance that originated a message is not available, a different Email Security appliance can process and deliver released messages. You designate the appliance for this purpose.

Before you begin

- Verify that the alternate appliance can process and deliver released messages as expected. For example, configurations for encryption and antivirus rescanning should match the same configurations on your primary appliances.
- The alternate appliance must be fully configured for centralized policy, virus, and outbreak quarantines. Complete the steps in the table in [Centralizing Policy, Virus, and Outbreak Quarantines](#) , on page 305 for that appliance.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 Click the **Specify Alternate Release Appliance** button.

Step 4 Choose an Email Security appliance.

Step 5 Submit and commit your changes.

What to do next**Related Topics**

[Releasing Messages When an Email Security Appliance Is Unavailable](#) , on page 311

Configuring Centralized Quarantine Access for Custom User Roles

In order to allow administrators with custom user roles to specify centralized policy quarantines in message and content filters and in DLP message actions on the Email Security appliance, you must grant those users access to the relevant policy quarantines on the Security Management appliance, and the custom user role names that you create on the Security Management appliance must match those on the Email Security appliance.

Related Topics

- [Creating Custom Email User Roles](#) , on page 409

Disabling Centralized Policy, Virus, and Outbreak Quarantines

Generally, if you need to disable these centralized quarantines, you should do so on the Email Security appliance.

For information about disabling centralized policy, virus, and outbreak quarantines, including a list of impacts of doing so, see the online help or documentation for your Email Security appliance.

Releasing Messages When an Email Security Appliance Is Unavailable

Normally, when a message is released from a centralized quarantine, the Security Management appliance returns it for processing to the Email Security appliance that originally sent it to the centralized quarantine.

If the Email Security appliance that originated a message is not available, a different Email Security appliance can process and deliver released messages. You should designate an alternate release appliance for this purpose.

If the alternate appliance is unavailable, you can specify a different Email Security appliance as the alternate release appliance and that appliance will process and deliver queued messages.

After repeated unsuccessful attempts to reach an Email Security appliance, you will receive an alert.

Related Topics

- [Designating an Alternate Appliance to Process Released Messages](#), on page 310

Managing Policy, Virus, and Outbreak Quarantines

- [Disk Space Allocation for Policy, Virus, and Outbreak Quarantines](#) , on page 312
- [Retention Time for Messages in Quarantines](#) , on page 312
- [Default Actions for Automatically Processed Quarantined Messages](#) , on page 313
- [Checking the Settings of System-Created Quarantines](#) , on page 314
- [Configuring Policy, Virus, and Outbreak Quarantines](#) , on page 314
- [About Editing Policy, Virus, and Outbreak Quarantine Settings](#) , on page 316
- [Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned](#) , on page 316
- [About Deleting Policy Quarantines](#) , on page 316

- [PVO Quarantine Threshold Alert](#) , on page 317
- [Monitoring Quarantine Status, Capacity, and Activity](#) , on page 318
- [Alerts About Quarantine Disk-Space Usage](#) , on page 320
- [Policy Quarantines and Logging](#), on page 320
- [About Distributing Message Processing Tasks to Other Users](#) , on page 320

Disk Space Allocation for Policy, Virus, and Outbreak Quarantines

For information about allocating disk space, see [Managing Disk Space](#) , on page 521.

Messages in multiple quarantines consume the same amount of disk space as a message in a single quarantine.

If Outbreak Filters and Centralized Quarantines are both enabled:

- All disk space on the appliance that would have been allocated to local policy, virus, and outbreak quarantines is used instead to hold copies of messages in the Outbreak quarantine, in order to scan those messages each time outbreak rules are updated.
- The disk space on the Security Management appliance for messages in the Outbreak quarantine from a particular managed Email Security appliance may be limited by the amount of available disk space for quarantined messages on that Email Security appliance.
- For more information about this situation, see [Retention Time for Messages in Quarantines](#) , on page 312

Related Topics

- [Monitoring Quarantine Status, Capacity, and Activity](#) , on page 318
- [Alerts About Quarantine Disk-Space Usage](#) , on page 320
- [Retention Time for Messages in Quarantines](#) , on page 312

Retention Time for Messages in Quarantines

Messages are automatically removed from the quarantine under the following circumstances:

- Normal Expiration—the configured retention time is met for a message in the quarantine. You specify a retention time for messages in each quarantine. Each message has its own specific expiration time, displayed in the quarantine listing. Messages are stored for the amount of time specified unless another circumstance described in this topic occurs.



Note The normal retention time for messages in the Outbreak Filters quarantine is configured in the Outbreak Filters section of each mail policy, not in the outbreak quarantine.

- Early Expiration—messages are forced from quarantines before the configured retention time is reached. This can happen when:
 - The size limit for all quarantines, as defined in [Disk Space Allocation for Policy, Virus, and Outbreak Quarantines](#) , on page 312, is reached.

If the size limit is reached, the oldest messages, regardless of quarantine, are processed and the default action is performed for each message, until the size of all quarantines is again less than the

size limit. The policy is First In First Out (FIFO). Messages in multiple quarantines will be expired based on their latest expiration time.

(Optional) You can configure individual quarantines to be exempt from release or deletion because of insufficient disk space. If you configure all quarantines to be exempt and the disk space reaches capacity messages will be held on the Email Security appliance until space is available on the Security Management appliance.

Because the Security Management appliance does not scan messages, a copy of each message in the centralized outbreak quarantine is stored on the Email Security appliance that originally processed the message. This allows the Email Security appliance to rescan quarantined messages each time outbreak filter rules are updated, and tell the Security Management appliance to release messages that are no longer deemed a threat. Both copies of the outbreak quarantine should hold the same set of messages at all times. Therefore, in the rare situation when disk space on the Email Security appliance becomes full, then the copies of messages in the Outbreak quarantine on both appliances will expire early, even if the centralized quarantine still has space.

You will receive alerts at disk-space milestones. See [Alerts About Quarantine Disk-Space Usage](#), on page 320.

- You delete a quarantine that still holds messages.

When a message is automatically removed from a quarantine, the default action is performed on that message. See [Default Actions for Automatically Processed Quarantined Messages](#), on page 313.



Note In addition to the above scenarios, messages can be automatically removed from quarantine based on the result of scanning operations (outbreak filters or file analysis.)

Effects of Time Adjustments on Retention Time

- Daylight savings time and appliance time zone changes do not affect the retention period.
- If you change the retention time of a quarantine, only new messages will have the new expiration time.
- If the system clock is changed, messages that should have expired in the past will expire at the next most appropriate time.
- System clock changes do not apply to messages that are in the process of being expired.

Default Actions for Automatically Processed Quarantined Messages

The default action is performed on messages in a policy, virus, or outbreak quarantine when any situation described in [Retention Time for Messages in Quarantines](#), on page 312, occurs.

There are two primary default actions:

- Delete—The message is deleted.
- Release—The message is released for delivery.

Upon release, messages may be rescanned for threats. For more information, see [About Rescanning of Quarantined Messages](#), on page 327.

In addition, messages released before their expected retention time has passed can have additional operations performed on them, such as adding an X-Header. For more information, see [Configuring Policy, Virus, and Outbreak Quarantines](#), on page 314.

Messages released from a centralized quarantine are returned to the originating Email Security appliance for processing.

Checking the Settings of System-Created Quarantines

Before you use quarantines, customize the settings of the default quarantines, including the Unclassified quarantine.

Related Topics

- [Configuring Policy, Virus, and Outbreak Quarantines](#) , on page 314

Configuring Policy, Virus, and Outbreak Quarantines

Before you begin

- If you are editing an existing quarantine, see [About Editing Policy, Virus, and Outbreak Quarantine Settings](#) , on page 316.
- Understand how messages in quarantines are automatically managed, including retention times and default actions. See [Retention Time for Messages in Quarantines](#) , on page 312, and [Default Actions for Automatically Processed Quarantined Messages](#) , on page 313.
- Determine which users you want to have access to each quarantine, and create users and custom user roles accordingly. For details, see [Which User Groups Can Access Policy, Virus, and Outbreak Quarantines](#) , on page 321.

Step 1 You can configure Policy, Virus, and Outbreak Quarantines in any one of the following ways:

- [New Web Interface Only] Choose **Quarantine > Other Quarantine > View > +**.
- Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines** and do one of the following:
 - Click **Add Policy Quarantine**.
 - Click a quarantine to edit.

Step 2 Enter the following information:

Keep the following in mind:

- Changing the retention time of the File Analysis quarantine from the default of one hour is not recommended.
- If you do *not* want messages in this quarantine to be processed before the end of the Retention Period you specify, even when quarantine disk space is full, deselect **Free up space by applying default action on messages upon space overflow**.

Do not select this option for all quarantines. The system must be able to make space by deleting messages from at least one quarantine.

- If you select **Release** as the default action, you can specify additional actions to apply to messages that are released before their retention period has passed:

Option	Information
Modify Subject	Type the text to add and specify whether to add it to the beginning or the end of the original message subject. For example, you might want to warn the recipient that the message may contain inappropriate content. Note In order for a subject with non-ASCII characters to display correctly it must be represented according to RFC 2047.
Add X-Header	An X-Header can provide a record of actions taken on a message. This can be helpful for example when handling inquiries about why a particular message was delivered. Enter a name and value. Example: Name = Inappropriate-release-early Value = True
Strip Attachments	Stripping attachments protects against viruses that may be in such files.

Step 3 Specify the users who can access this quarantine:

User	Information
Local Users	The list of local users includes only users with roles that can access quarantines. The list excludes users with Administrator privileges, because all Administrators have full access to quarantines.
Externally Authenticated Users	You must have configured external authentication.
Custom User Roles	You see this option only if you have created at least one custom user role with quarantine access.

Step 4 Submit and commit your changes.

What to do next

See [Message Filters Page, on page 145](#) and [Content Filters Page, on page 146](#)

- If you have not yet migrated quarantines from the Email Security appliance:

You will assign these quarantines to message and content filters and DLP message actions as part of the migration process.

- If you have already migrated to centralized quarantines:

Make sure your Email Security appliance has message and content filters and DLP message actions that will move messages to the quarantine. See the user guide or online help for the Email Security appliance.

About Editing Policy, Virus, and Outbreak Quarantine Settings




Note

- You cannot rename a quarantine.
- See also [Retention Time for Messages in Quarantines](#) , on page 312.

To change quarantine settings, choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**, and then click the name of a quarantine.


To change quarantine settings on the new web interface, navigate to **Quarantine > Other Quarantine >**

View and click  on the required quarantine or

To change quarantine settings on the legacy web interface, choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**, and then click the name of a quarantine.

Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned

You can view the message filters, content filters, Data Loss Prevention (DLP) message actions, and DMARC verification profiles that are associated with a policy quarantine, and the Email Security appliance on which each is configured.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click on **Quarantine > Other Quarantine > View**.
- Step 2** [New Web Interface Only] Select the required quarantine and click on the  button.
- Step 3** Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**.
- Step 4** Click the name of the policy quarantine to check.
- Step 5** Scroll to the bottom of the page and view the **Associated Message Filters/Content Filters/DLP Message Actions**.
-

About Deleting Policy Quarantines

- Before you delete a policy quarantine, see if it is associated with any active filters or message actions. See [Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned](#) , on page 316.
- You can delete a policy quarantine even if it is assigned to a filter or message action.
- If you delete a quarantine that is not empty, the default action defined in the quarantine will be applied to all messages, even if you have selected the option not to delete messages if the disk is full. See [Default Actions for Automatically Processed Quarantined Messages](#) , on page 313.
- After you delete the quarantine associated with a filter or message action, any messages subsequently quarantined by that filter or message action will be sent to the Unclassified quarantine. You should customize the default settings of the Unclassified quarantine before you delete quarantines.
- You cannot delete the Unclassified quarantine.

PVO Quarantine Threshold Alert

Secure Email and Web Manager sends an alert to the recipient when the number of PVO quarantine messages exceeds a user-defined threshold value set for a specific time duration and PVO quarantine. Secure Email and Web Manager ensures that you receive the alerts you set as an email.

You can configure the PVO quarantine threshold alert using CLI or the web interface.

Related Topics

- [Configuring PVO Quarantine Threshold Alert Settings using CLI, on page 317](#)
- [Configuring PVO Quarantine Threshold Alert Settings using Web Interface, on page 317](#)

Configuring PVO Quarantine Threshold Alert Settings using CLI

To configure PVO quarantine threshold alerts, use the `quarantineconfig` command in the CLI. When you execute the command, you are prompted to enable or disable PVO quarantine threshold alert. By default, the PVO quarantine threshold alert is disabled. You must provide values for the following parameters:

- **Threshold:** configures the threshold value. If the number of PVO quarantine messages exceeds this value, Secure Email and Web Manager sends an alert to the recipient. This value can be configured for each quarantine policy. The value ranges from 1 to 10,00,000.
- **Duration:** configures the time duration (in hours) during which the Secure Email and Web Manager must count the number of PVO quarantine messages in each quarantine. The value ranges from 0.5 to 24. You can configure the value of duration only in multiples of 0.5 (0.5, 1, 1.5, and so on).
- **Alert Limit:** configures the alert limit. This value indicates the number of alerts the Secure Email and Web Manager sends to the recipient for the configured time duration. This value is set for each quarantine policy. The value ranges from 1 to 20.

Procedure

Command or Action	Purpose
<code>quarantineconfig</code>	This command configures the PVO quarantine threshold alert.

Configuring PVO Quarantine Threshold Alert Settings using Web Interface

You can configure PVO quarantine threshold alerts using the web interface of Secure Email and Web Manager.

Before you begin

Make sure you have met the following prerequisites to receive the PVO quarantine threshold alerts:

- Configured System Alerts.
- Enabled System - Critical Alerts.

Step 1 [New Web Interface Only] Click  on Secure Email and Web Manager to load the legacy web interface.

Step 2 Go to **Email > Message Quarantine > Policy Virus and Outbreak Quarantines** page.

The **Policy, Virus and Outbreak Quarantines** page is displayed. The **Quarantines** window displays all the PVO Quarantines.

Step 3 Click **Add Policy Quarantine** to add a new PVO quarantine or click an existing PVO quarantine to edit the PVO quarantine.

For more information on adding and editing a PVO quarantine, see [Configuring Policy, Virus, and Outbreak Quarantines](#), on page 314 section.

Step 4 Select the **Enable Threshold Alert** checkbox in the **Threshold Alert Settings** window.


Step 5 Enter the values for the following fields in the **Threshold Alert Settings** window.




- Threshold
- Time duration
- Alert Limit


For more details on the parameter values, see [Configuring PVO Quarantine Threshold Alert Settings using CLI](#), on page 317 section.

Step 6 Submit and commit your changes.

Monitoring Quarantine Status, Capacity, and Activity

To View	Do This
Total space allocated for all non-spam quarantines	<p>[New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.</p> <p>Choose Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines and look in the first section on the page.</p> <p>To change allocations, see Managing Disk Space, on page 521.</p>
Currently available space for all non-spam quarantines	<p>[New Web Interface Only] Choose Quarantine > Other Quarantine.</p> <p>or</p> <p>Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines and look just below the table.</p> <p>The available space for policy, virus and outbreak quarantine is displayed above the table in the Quarantines section</p>

To View	Do This
Total amount of space currently used by all quarantines	<p>[New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.</p> <p>Choose Management Appliance > Centralized Services > System Status.</p>
Amount of space currently used by each quarantine	<p>[New Web Interface Only] Choose Quarantines Quarantine > Other Quarantine > View.</p> <p>The table displays the amount of space currently used by each quarantine.</p> <p>or</p> <p>Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines, click the quarantine name, and look for this information in the table row directly below the quarantine name.</p>
Total number of messages currently in all quarantines	<p>[New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.</p> <p>Choose Management Appliance > Centralized Services > System Status.</p>
Number of messages currently in each quarantine	<p>[New Web Interface Only] Choose Quarantines Quarantine > Other Quarantine > View.</p> <p>The table displays the total number of messages currently available for each quarantine.</p> <p>or</p> <p>Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines and look at the table row for the quarantine.</p>
Total CPU usage by all quarantines	<p>[New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.</p> <p>Choose Management Appliance > Centralized Services > System Status and look in the System Information section.</p>
Date and time when the last message entered each quarantine (excluding moves between policy quarantines)	<p>[New Web Interface Only] Choose Quarantines > Other Quarantine > View.</p> <p>The table displays the date and time when the last message was quarantined.</p> <p>or</p> <p>Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines and look at the table row for the quarantine.</p>

To View	Do This
Date a policy quarantine was created	[New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface. Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines , click the quarantine name, and look for this information in the table row directly below the quarantine name. Creation date and creator name are not available for system-created quarantines.
Name of policy quarantine creator	
Filters and message actions associated with a policy quarantine	See Determining the Filters and Message Actions to Which a Policy Quarantine Is Assigned , on page 316.

Alerts About Quarantine Disk-Space Usage

An alert is sent whenever the total size of the policy, virus, and outbreak quarantine reaches or passes 75 percent, 85 percent, and 95 percent of its capacity. The check is performed when a message is placed in the quarantine. For example, if adding a message to a quarantine increases the size to or past 75 percent of the total capacity, an alert is sent.

Policy Quarantines and Logging

AsyncOS individually logs all messages that are quarantined:

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

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

AsyncOS also individually logs messages that are removed from quarantine:

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

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

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

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

When a message is re-injected, the system creates a new Message object with a new Message ID (MID). This is logged using an existing log message with a new MID “byline”, for example:

Info: MID 483 rewritten to 513 by Policy Quarantine

About Distributing Message Processing Tasks to Other Users

You can distribute message review and processing tasks to other administrative users. For example:

- The Human Resources team can review and manage the Policy Quarantine.

- The Legal team can manage the Confidential Material Quarantine.

You assign access privileges to these users when you specify settings for a quarantine. In order to add users to quarantines, the users must already exist.

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

Related Topics

- [Which User Groups Can Access Policy, Virus, and Outbreak Quarantines](#) , on page 321
- [Distributing Administrative Tasks](#), on page 403

Which User Groups Can Access Policy, Virus, and Outbreak Quarantines

When you allow administrative users to access a quarantine, the actions that they can perform depend on their user group:

- Users in the Administrators or Email Administrators groups can create, configure, delete, and centralize quarantines and can manage quarantined messages.
- Users in the Operators, Guests, Read-Only Operators, and Help Desk Users groups, as well as custom user roles with quarantine management privileges, can search for, view, and process messages in a quarantine, but cannot change the quarantine's settings, create, delete, or centralize quarantines. You specify in each quarantine which of these users have access to that quarantine.
- Users in the Technicians group cannot access quarantines.

Access privileges for related features, such as Message Tracking and Data Loss Prevention, also affect the options and information that an administrative user sees on Quarantine pages. For example, if a user does not have access to Message Tracking, that user will not see message tracking information for quarantined messages.

Note: To allow custom user roles configured on the Security Management appliance to specify policy quarantines in filters and DLP message actions, see [Configuring Centralized Quarantine Access for Custom User Roles](#) , on page 311.


End users do not have see or have access to policy, virus, and outbreak quarantines.

Working with Messages in Policy, Virus, or Outbreak Quarantines

Related Topics

- [Viewing Messages in Quarantines](#) , on page 322
- [Searching for Messages in Policy, Virus, and Outbreak Quarantines](#) , on page 323
- [Manually Processing Messages in a Quarantine](#), on page 323
- [Messages in Multiple Quarantines](#) , on page 325
- [Message Details and Viewing Message Content](#), on page 325
- [About Rescanning of Quarantined Messages](#) , on page 327
- [The Outbreak Quarantine](#), on page 328

Viewing Messages in Quarantines

To	Do This
View all messages in a quarantine	[New Web Interface Only] Choose Quarantine > Other Quarantine > View . or Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines . In the row for the relevant quarantine, click the blue number in the Messages column of the table.
View messages in the Outbreak quarantine	[New Web Interface] Choose Quarantine > Other Quarantine > View . or Choose Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines . In the row for the relevant quarantine, click the blue number in the Messages column of the table. See Manage by Rule Summary Link, on page 329 or Rule Summary View, on page 328 [New Web Interface Only].
Navigate through the list of messages in a quarantine	Click Previous, Next, a page number, or double-arrow link. The double arrows take you to the first (<<) or last (>>) page in the listing. [New Web Interface Only] Scroll down on the table to display details of all the new messages.
Sort the list of messages in a quarantine	Click a column heading (except columns that could include multiple items or the “In quarantines” column).
Resize table columns	Drag the divider between column headings.
Customize table columns	Click  and select the columns to display, and click Close
View the content that caused the message to be quarantined	See Viewing Matched Content , on page 326.

Related Topics

- [Quarantined Messages and International Character Sets, on page 322](#)

Quarantined Messages and International Character Sets

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

Searching for Messages in Policy, Virus, and Outbreak Quarantines

**Note**

- Users can find and see only the messages in quarantines to which they have access.
- Searches in Policy, Virus, and Outbreak quarantines do not find messages in the spam quarantine.

Step 1 [New Web Interface Only] Choose **Quarantine > Other Quarantine > Search**.

Step 2 [New Web Interface Only] Click the blue number link of the corresponding quarantine.

Tip [New Web Interface Only] For the Outbreak Quarantine, you can also find all messages quarantined by each outbreak rule: Click the **Rule Summary** tab in the Outbreak quarantine, and then click the relevant rule.

Step 3 Choose **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines**.

Step 4 Click the **Search Across Quarantines** button.

Tip For the Outbreak Quarantine, you can also find all messages quarantined by each outbreak rule: Click the **Manage by Rule Summary** link in the Outbreak table row, and then click the relevant rule.

Step 5 (Optional) Enter other search criteria.

- For Envelope Sender and Envelope Recipient: You can enter any character(s). No validation of your entry is performed.
- Search results include only messages that match *all* of the criteria you specify. For example, if you specify an Envelope Recipient and a Subject, only messages that match the terms specified in both the Envelope Recipient *and* the Subject are returned.

What to do next

You can use the search results in the same way that you use the quarantine listings. For more information, see [Manually Processing Messages in a Quarantine, on page 323](#).

For information on modifying your search criteria, see [Modifying Search Criteria, on page 323](#).

Modifying Search Criteria






You can modify the search criteria to a custom time range or a different quarantine.

To modify the search criteria, click **Modify**.

Manually Processing Messages in a Quarantine

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

You can perform the following actions on messages:

- Delete 
- Release 
- Delay Scheduled Exit from quarantine 
- Send a Copy of messages to email addresses that you specify 
- Move a message from one quarantine to another 

Generally, you can perform actions on messages in the lists that are displayed when you do the following. However, not all actions are available in all situations.

- From the list of quarantines on the **Email > Message Quarantine > Policy, Virus, and Outbreak Quarantines** page or [New Web Interface Only] **Quarantine > Other Quarantine > View** page, click the number of messages in a quarantine.
- Click on the check box of the quarantine message and select the required actions.

You can perform these actions on multiple messages at one time by:

- Choosing an option from the pick list at the top of the list of messages.
- Selecting the check box beside each message listed on a page.
- Selecting the check box in the table heading at the top of a list of messages. This applies the action to all messages visible on the screen. Messages on other pages are not affected.

Additional options are available for messages in the outbreak quarantine. See information about the Rule Summary view in the chapter on Outbreak Filters in the online help or user guide for the *AsyncOS for Email Security Appliances*.

Related Topics

- [Sending a Copy of the Message, on page 324](#)
- [About Moving Messages Between Policy Quarantines , on page 324](#)
- [Messages in Multiple Quarantines , on page 325](#)
- [Default Actions for Automatically Processed Quarantined Messages , on page 313](#)

Sending a Copy of the Message

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

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

About Moving Messages Between Policy Quarantines

You can manually move messages from one policy quarantine to another on a single appliance .

When you move a message to a different quarantine:

- The expiration time is unchanged. The message keeps the retention time of the original quarantine.

- The reason the message was quarantined, including the matched content and other relevant details, does not change.
- If a message is in multiple quarantines and you move the message to a destination that already holds a copy of that message, the expiration time and reason for quarantine of the moved copy of the message overwrite those of the copy of the message that was originally in the destination quarantine.

Messages in Multiple Quarantines

If a message is present in one or more other quarantines, the “In other quarantines” column in the quarantine message list will show “Yes,” regardless of whether you have permissions to access those other quarantines.

A message in multiple quarantines:

- Is not delivered unless it has been released from all of the quarantines in which it resides. If it is deleted from any quarantine, it will never be delivered.
- Is not deleted from any quarantine until it has been deleted or released from all quarantines in which it resides.

Because a user wanting to release a message may not have access to all of the quarantines in which it resides, the following rules apply:

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

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

- The user will be informed whether the message is present in each of the quarantines to which the user has access.
- The GUI shows only the scheduled exit time from the quarantines to which the user has access. (For a given message, there is a separate exit time for each quarantine.)
- The user will not be told the names of the other quarantine(s) holding the message.
- The user will not see matched content that caused the message to be placed into quarantines that the user does not have access to.
- Releasing a message affects only the queues to which the user has access.
- If the message is also queued in other quarantines not accessible to the user, the message will remain in quarantine, unchanged, until acted upon by users who have the required access to the remaining quarantines (or until the message is released “normally” via early or normal expiration).

Message Details and Viewing Message Content

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

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

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

The Message Details section displays the message body, message headers, and attachments. Only the first 100 K of the message body is displayed. If the message is longer, the first 100 K is shown, followed by an

ellipsis (...). The actual message is not truncated. This is for display purposes only. You can download the message body by clicking [message body] in the Message Parts section at the bottom of Message Details. You can also download any of the message's attachments by clicking the attachment's filename.



Note The maximum limit for the attachment downloads on the Message Details page is restricted to 25 MB.

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

To view additional details about the message, click the **Message Tracking** link.



Note For the special Outbreak quarantine, additional functionality is available. See [The Outbreak Quarantine, on page 328](#).

Related Topics

- [Viewing Matched Content](#) , on page 326
- [Downloading Attachments](#) , on page 327

Viewing Matched Content

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

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

When you view messages in the local quarantine that have triggered message or content filter rules, the GUI may display content that did not actually trigger the filter action (along with content that triggered the filter action). The GUI display should be used as a guideline for locating content matches, but does not necessarily reflect an exact list of content matches. This occurs because the GUI uses less strict content matching logic than is used in the filters. This issue applies only to the highlighting in the message body. The table that lists the matched strings in each part of the message, along with the associated filter rule, is correct.

Figure 5: Matched Content Viewed in the Policy Quarantine

The screenshot displays the 'Matched Content' interface. At the top, there is a 'Policy' dropdown menu. Below it is a table with columns for 'Attachment Name', 'Matched Content', and 'Condition'. The first row shows an attachment named 'FP1.1.txt' with a condition of 'DLP Classifier: Contact Information'. The 'Matched Content' column contains a list of email addresses and company information.

Below the table is the 'Headers' section, which displays the following text:

```
X-IronPort-AV: E=Sophos;i="4.43,282,1246818600";
d="txt?scan'208";a="178202"
Received: from d2.vmw023-bsd04.ibqa (HELO vmw023-bsd04.ibqa) ([172.22.107.1])
by c360a02.ibqa with ESMTP; 28 Jul 2009 16:25:03 +0530
Message-ID: <792087.518002035-sendEmail@vmw023-bsd04>
From: "user@test.com" <user@test.com>
To: "user1@test.com" <user1@test.com>
Subject: DLPTEST
Date: Tue, 28 Jul 2009 08:42:11 +0000
X-Mailer: sendEmail-1.55
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----MIME delimiter for sendEmail-538525.714612664"
```

Below the headers is the 'Message' section, which contains the text 'Test'.

At the bottom is the 'Message Parts' section, which contains a table with the following data:

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

Downloading Attachments

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

About Rescanning of Quarantined Messages

When a message is released from all queues in which it has been quarantined, the following rescanning occurs, depending on the features enabled for the appliance and for the mail policy that originally quarantined the message:

- Messages released from Policy and Virus quarantines are rescanned by the anti-virus, advanced malware protection, and graymail engines.
- Messages released from the Outbreak quarantine are rescanned by the anti-spam, AMP, and anti-virus engines.
- Messages released from the File Analysis quarantine are rescanned for threats.
- Messages with attachments are rescanned by the file reputation service upon release from Policy, Virus, and Outbreak quarantines.

Upon rescanning, if the verdict produced matches the verdict produced the previous time the message was processed, the message is not re-quarantined. Conversely, if the verdict is different, the message could be sent to another quarantine.

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

The Outbreak Quarantine

The Outbreak quarantine is present when a valid Outbreak Filters feature license key has been entered. The Outbreak Filters feature sends messages to the Outbreak quarantine, depending on the threshold set. For more information, see the Outbreak Filters chapter in the online help or user guide for the Email Security appliance.

The Outbreak quarantine functions just like other quarantines—you can search for messages, release or delete messages, and so on.

The Outbreak quarantines has the following views:

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

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

Related Topics

- [Rescanning Messages in an Outbreak Quarantine](#) , on page 328
- [Rule Summary View](#), on page 328
- [Reporting False Positives or Suspicious Messages to Cisco Systems](#), on page 329

Rescanning Messages in an Outbreak Quarantine

Messages placed in the Outbreak quarantine are automatically released if newly published rules deem the quarantined message no longer a threat.

If anti-spam and anti-virus are enabled on the appliance , the scanning engines scan every message released from the Outbreak quarantine based on the mail flow policy that applies to the message.

Rule Summary View

The Rule Summary view is available only in the new web interface.

In the Outbreak quarantine, click the **Rule Summary** tab to see the listing of the contents of Outbreak quarantine, grouped by Rule ID.

You can perform message actions (Release and Delete) on all of the messages in the quarantine based on which outbreak rule caused the message to be quarantined. This is ideal for clearing out large numbers of messages from the Outbreak quarantine. For more information, see Outbreak Quarantine and the Manage by Rule Summary View section of chapter “Outbreak Filters” in the online help or user guide of the *AsyncOS for the Email Security Appliance*.

Manage by Rule Summary Link

Click the Manage by Rule Summary link next to the Outbreak quarantine in the quarantine listing to view the Manage by Rule Summary page. You can perform message actions (Release, Delete, Delay Exit) on all of the messages in the quarantine based on which outbreak rule caused the message to be quarantined. This is ideal for clearing out large numbers of messages from the Outbreak quarantine. For more information, see information about the Manage by Rule Summary view in the Outbreak Filters chapter in the online help or user guide for the Email Security appliance

Reporting False Positives or Suspicious Messages to Cisco Systems

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

Step 1 Navigate to a message in the Outbreak quarantine.

Step 2 Enter the recipient address and click **Send**.

Troubleshooting Centralized Policy Quarantines

- [Administrative User Cannot Choose Quarantines in Filters and DLP Message Actions](#), on page 329
- [Messages Released from a Centralized Outbreak Quarantine Are Not Rescanned](#), on page 329

Administrative User Cannot Choose Quarantines in Filters and DLP Message Actions

Problem

Administrative users cannot see or choose quarantines in content and message filters or DLP actions on the Email Security appliance.

Solution

See [Configuring Centralized Quarantine Access for Custom User Roles](#), on page 311

Messages Released from a Centralized Outbreak Quarantine Are Not Rescanned

Problem

Messages released from the Outbreak Quarantine should be scanned again before delivery. However, some contaminated messages have been delivered from the quarantine.

Solution

This can occur under the situation described in [About Rescanning of Quarantined Messages](#), on page 327

Messages Released from a Centralized Outbreak Quarantine Are Not Rescanned



CHAPTER 11

Managing Web Security Appliances

This chapter contains the following sections:

- [About Centralized Configuration Management](#) , on page 331
- [Determining the Correct Configuration Publishing Method](#) , on page 332
- [Using Configuration Masters to Centrally Manage Web Security Appliances](#) , on page 332
- [Initializing and Configuring Configuration Masters](#), on page 336
- [Setting Up to Use Advanced File Publishing](#) , on page 346
- [Publishing Configurations to Web Security Appliances](#), on page 346
- [Viewing Status and History of Publishing Jobs](#) , on page 351
- [Centralized Upgrade Management](#), on page 352
- [Viewing Web Security Appliance Status](#), on page 356
- [Preparing For and Managing URL Category Set Updates](#) , on page 358
- [Application Visibility and Control \(AVC\) Updates](#) , on page 360
- [Updating WBRS and AVC Data using CLI](#), on page 360
- [Troubleshooting Configuration Management Issues](#) , on page 360

About Centralized Configuration Management

Centralized configuration management allows you to publish configurations from a Cisco Secure Email and Web Manager appliance to the associated Web Security appliances, in order to:

- Simplify and speed management of web security policies by configuring or updating settings once on the Security Management appliance, instead of on each Web Security appliance.
- Ensure uniform policy enforcement across distributed networks.

There are two ways to publish settings to Web Security appliances:

- Using Configuration Masters
- Using configuration files from Web Security appliances (using Advanced File Publishing)

Determining the Correct Configuration Publishing Method

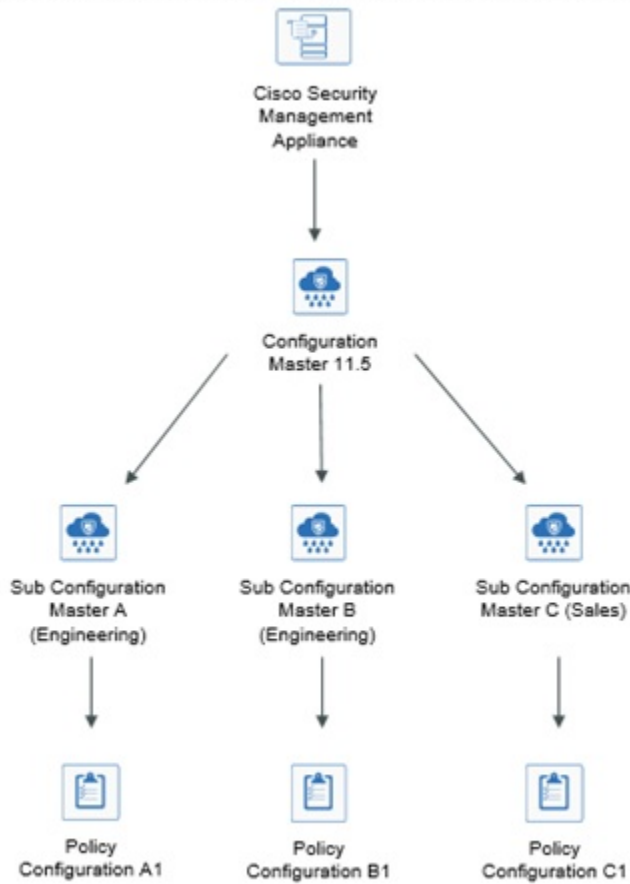
There are two different processes for publishing configurations from the Secure Email and Web Manager appliance, and each publishes different settings. Some settings cannot be centrally managed.

To Configure	Do This
<p>Features that appear under the Web Security Manager menu on the Web Security appliance, such as policies and custom URL categories.</p> <p>Exception: L4 Traffic Monitor (L4TM) settings are not included in Configuration Masters.</p> <p>The exact features supported depend on the configuration master version, which corresponds to an AsyncOS for Web Security version.</p>	<p>Publish a Configuration Master.</p> <p>Many features that are configurable in a Configuration Master also require configurations directly on the Web Security appliance in order to work. For example, SOCKS Policies are configurable via Configuration Master, but a SOCKS Proxy must first be configured directly on the Web Security appliance.</p>
<p>Note: Integration with a Cisco Identity Services Engine (ISE) must be configured independently on each Web Security appliance. Cisco Identity Services Engine settings cannot be published from a Cisco Secure Email and Web Manager appliance.</p>	<p>Use Advanced File Publishing.</p>
<p>FIPS mode for Federal Information Processing Standard, Network/interface settings, DNS, Web Cache Communication Protocol (WCCP), upstream proxy groups, certificates, the proxy mode, time settings such as NTP, L4 Traffic Monitor (L4TM) settings, and authentication redirect hostname.</p>	<p>Configure settings directly on your managed Web Security appliances.</p> <p>See the AsyncOS for Cisco Web Security Appliances User Guide</p>

Using Configuration Masters to Centrally Manage Web Security Appliances

Your Security Management appliance provides different versions of Configuration Masters, so that you can centrally manage your Web Security appliances. Each Configuration Master supports multiple sub Configuration Masters under it. The sub configuration masters allows you to define different policy configurations within the same configuration master.

Assume that your engineering and sales teams are using AsyncOS 11.7 for Web Security appliances. Your organizational policy requires you define different policies for these teams. In this scenario, you can create two sub configuration masters under the Configuration Master 11.7 and define different policy configurations for each sub configuration master, as shown in the following figure:



Setting Up Configuration Masters to Centrally Manage Web Security Appliances

The following table provides instructions to initialize and configure Configuration Masters and sub configuration masters.

Steps	Do This	On This Appliance	More Information
Step 1	Check for general configuration requirements and caveats.	—	See Important Notes About Using Configuration Masters , on page 335.
Step 2	Determine the Configuration Master version to use for each Web Security appliance.	—	See Determine the Configuration Master Versions to Use , on page 335.
Step 3	On all target Web Security appliances, enable and configure the features and functionality that are required to support the policy and other settings that you will configure in Configuration Masters on the Security Management appliance.	Web Security appliances	—

Steps	Do This	On This Appliance	More Information
Step 4	(Optional) If you have a working Web Security appliance that can serve as a configuration model for all of your Web Security appliances, you can use a configuration file from that Web Security appliance to speed configuration of a Configuration Master in the Security Management appliance.	Web Security appliance	For instructions on downloading a configuration file from a Web Security appliance, see “Saving and Loading the Appliance Configuration” in the AsyncOS for Cisco Web Security Appliances User Guide.
Step 5	Enable and configure Centralized Configuration Management.	Security Management appliance	See Enabling Centralized Configuration Management on the Security Management Appliance , on page 335.
Step 6	Initialize the Configuration Masters.	Security Management appliance	See Initializing and Configuring Configuration Masters , on page 336.
Step 7	(Optional) Configure Sub Configuration Masters	Security Management appliance	See Configuring Sub Configuration Masters , on page 338
Step 8	(Optional) Select the Sub Configuration Master as the Active Configuration	Security Management appliance	See Selecting the Sub Configuration Master as the Active Configuration , on page 339
Step 9	Associate Web Security appliances to the Configuration Masters.	Security Management appliance	See About Associating Web Security Appliances to Configuration Masters , on page 336.
Step 10	Import and/or manually configure policies, custom URL categories, and/or a web proxy bypass list in the Configuration Masters.	Security Management appliance	See Configuring Settings to Publish , on page 340
Step 11	Ensure that the features enabled on each Web Security appliance match the features enabled for the Configuration Master assigned to that appliance.	Security Management appliance	See Ensuring that Features are Enabled Consistently , on page 343.
Step 12	After you have set up required Configuration Masters and enabled appropriate features, publish configurations to your Web Security appliances.	Security Management appliance	See Publishing a Configuration Master , on page 346.
Step 13	Prepare in advance for possible URL Category set updates that can modify your existing Configuration Master settings.	Security Management appliance	Preparing For and Managing URL Category Set Updates , on page 358

Important Notes About Using Configuration Masters



Important Before you upgrade to AsyncOS 12.0 and later, you may need to backup your Configuration Master setting. The Configuration Master versions 10.0 and earlier will be replaced with Configuration Master version 11.7 and later.

After you upgrade to this release, you must initialize new Configuration Masters or import the configurations from an existing Configuration Master. If you have an existing Configuration Master for a previous release (for example, 9.1), you can copy the settings to a new Configuration Master (for example, 11.5).

Due to the change in the Configuration Master version, the appliance list is lost from the Identities and Policies. You must re-associate the Web Security appliance in the Configuration Masters.



Note On each Web Security appliance that you will manage centrally, check to be sure that all Realm Names in Network > Authentication are unique across appliances, unless the settings for same-name realms are identical.

Determine the Configuration Master Versions to Use

Your Security Management appliance provides multiple Configuration Masters, so that you can centrally manage Web Security appliances that run different versions of AsyncOS for Web Security that support different features.

Each Configuration Master contains configurations to be used for a particular version or versions of AsyncOS for Web Security.

To determine which configuration master version to use for your versions of AsyncOS for Web Security, see the Compatibility Matrix at

<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>.



Note The Configuration Master version should match the AsyncOS version on the Web Security appliance, as specified in the Compatibility Matrix. Publishing an older Configuration Master version to a newer Web Security appliance may fail if settings on the Web Security appliance do not match the settings in the Configuration Master. This can occur even if the Web Appliance Status detail page does not indicate any discrepancies. In this case, you must manually compare the configurations on each appliance.

Enabling Centralized Configuration Management on the Security Management Appliance

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

Step 2 Click **Enable**.

- Step 3** If you are enabling Centralized Configuration Management for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.
- Step 4** Submit and commit your changes.

Initializing and Configuring Configuration Masters

- [Initializing Configuration Masters](#) , on page 336
- [Importing Settings from a Web Security Appliance](#) , on page 341
- [Configuring Settings to Publish](#) , on page 340

Initializing Configuration Masters

Note: After you initialize a configuration master, the Initialize option is not available. Instead, populate the Configuration Master using one of the methods described in [Configuring Settings to Publish](#) , on page 340 .

- Step 1** On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.
- 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**. You can also import settings from an existing Configuration Master later.
 - Otherwise, choose **Use default settings**.
- Step 4** Click **Initialize**.
- The Configuration Master is now available.
- Step 5** Repeat for each Configuration Master version to initialize.

About Associating Web Security Appliances to Configuration Masters

For information about compatibility of configuration masters with Web Security versions, see [Determine the Configuration Master Versions to Use](#), on page 335.

The simplest process for adding appliances to configuration masters depends on the situation:

If	Use This Procedure
You have not yet added Web Security appliances to the Security Management appliance	Adding Web Security Appliances and Associating Them with Configuration Master Versions , on page 337
You have already added Web Security appliances	Associating Configuration Masters to Web Security Appliances , on page 338
You want to view associated Configuration Masters in the appliance list	Viewing Associated Configuration Masters in the Appliance List , on page 339

Adding Web Security Appliances and Associating Them with Configuration Master Versions

Use this procedure if you have not yet added your Web Security appliances to be centrally managed.

Before you begin

- Choose the correct Configuration Master version for each Web Security appliance. See [Determine the Configuration Master Versions to Use, on page 335](#)
- Enable the following key exchange and cipher algorithms on the Web Security Appliance that you plan to add to the Security Management Appliance:

- Key Exchange Algorithms:

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1
```

- Cipher Algorithms:

```
3des-cbc,blowfish-cbc
```

To enable the algorithms, use the `sshconfig > sshd` command in CLI on the Web Security Appliance.

-
- Step 1** On the Security Management appliance, choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 2** Click **Add Web Appliance**.
- Step 3** In the Appliance Name and IP Address text fields, type the appliance name and the IP address or resolvable hostname for the Management interface of the Web Security appliance.
- Note** If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.
- Step 4** The Centralized Configuration Manager service is pre-selected.
- Step 5** Click **Establish Connection**.
- Step 6** Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.
- 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** Wait for the Success message to appear above the table on the page.
- Step 8** Choose the Configuration Master version to which you want to assign the appliance.
- Note** If you configure a subset of a particular version of configuration master and assign a Web Security appliance, then the sub configuration master version that is associated to the Web Security appliance is displayed in the drop-down list.
- Step 9** Submit and commit your changes.
- Step 10** Repeat this procedure for each Web Security Appliance for which you want to enable Centralized Configuration Management.
-

Associating Configuration Masters to Web Security Appliances

If you have already added Web Security appliances to the Security Management appliance, you can use the following procedure to quickly associate Web Security appliances with Configuration Master versions.

Before you begin

If you have not yet done so, choose the correct Configuration Master version for each Web Security appliance. See [Determine the Configuration Master Versions to Use, on page 335](#).

-
- Step 1** On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.
- Note** If a Configuration Master shows as Disabled, you can enable it by clicking **Web > Utilities > Security Services Display**, then **Edit Display Settings**. Select the check box for that Configuration Master to enable it. For more information, see [Enabling Features to Publish, on page 344](#).
- Step 2** Click **Security Appliances**.
- Step 3** Click on the required Web Security appliance.
- Step 4** Select the required configuration of the Configuration Master.
- You can see the different configurations of the Configuration Master in **Web > Utilities > Configuration Masters** page.
- Step 5** Submit and commit your changes.
-

Configuring Sub Configuration Masters

-
- Step 1** On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.
- Note** If a Configuration Master Setting shows as Disabled, you can enable it by clicking **Web > Utilities > Security Services Display**, then **Edit Display Settings**. Select the check box for that Configuration Master to enable it. For more information, see [Enabling Features to Publish, on page 344](#).
- Step 2** From the New Configuration Master page, click **New**.
- Step 3** Enter a unique name for the Configuration Master (for example, 11_5_new).
- Note** The name must contain only alphabets, numbers, and underscores. It cannot start with an underscore.
- Step 4** Select the Configuration Master version from the drop-down list.
- Step 5** For Select Configuration Source, select a Configuration Master from the dropdown-list.
- Step 6** Click **Submit** and commit your changes.
-

Viewing Associated Configuration Masters in the Appliance List

Before you begin

If you have not yet done so, choose the correct Configuration Master version for each Web Security appliance. See [Determine the Configuration Master Versions to Use](#), on page 335.

If you have already added Web Security appliances to the Security Management appliance, you can use the following procedure to view the associated Configuration Master versions in the Web Security appliance list.

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Note If a Configuration Master shows as Disabled, you can enable it by clicking **Web > Utilities > Security Services Display**, then **Edit Display Settings**. Select the check box for that Configuration Master to enable it. For more information, see [Enabling Features to Publish](#), on page 344.

Step 2 Click **Security Appliances**.

The Security Appliances page is same as the **Management Appliances > Centralized Services > Security Appliances** page. If you have added a Web Security appliance and associated configuration master to it, you can view the Configuration Master and AsyncOS version associated to the Web Security appliance.

Deleting Sub Configuration Masters

If you have configured sub configuration masters in [Configuring Sub Configuration Masters](#), on page 338, use the following procedure to delete the configurations.

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Note If a Configuration Master shows as Disabled, you can enable it by clicking **Web > Utilities > Security Services Display**, then **Edit Display Settings**. Select the check box for that Configuration Master to enable it. For more information, see [Enabling Features to Publish](#), on page 344.

Step 2 Click on the trash can icon on the required sub configuration master.

Note You cannot delete the configuration masters that are associated with a Web Security appliance.

Step 3 Submit and commit your changes.

Selecting the Sub Configuration Master as the Active Configuration

When you configure sub Configuration Masters, you must assign the required configuration as the active configuration.

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Step 2 Click **Edit** on the required configuration version of the Configuration Master. Selecting the configuration master version replaces the existing configuration of the Configuration Master.

Step 3 Commit your changes.

After you commit the changes, you can see the label of the Configuration Master drop down changed to the selected Configuration Master version.

Configuring Settings to Publish

Set up your configuration masters with the settings you want to publish.

There are several ways to set up Configuration Masters:

If	Do This
You are upgrading from a previous release of AsyncOS for Security Management and You did not initialize a new Configuration Master version by copying an earlier, existing Configuration Master into the new version	Import the old version. See Importing from an Existing Configuration Master , on page 340.
You have already configured a Web Security appliance and want to use those same configurations for multiple Web Security appliances	Import a configuration file that you saved from that Web Security appliance into the Configuration Master. You may have saved this configuration file when you reviewed Using Configuration Masters to Centrally Manage Web Security Appliances , on page 332. To import, see Importing Settings from a Web Security Appliance , on page 341.
You need to modify imported settings	See Configuring Web Security Features Directly in Configuration Masters , on page 341.
You have not yet configured policy settings, URL categories, or bypass settings on a Web Security appliance.	Configure these settings directly in an appropriate Configuration Master on the Security Management appliance. See Configuring Web Security Features Directly in Configuration Masters , on page 341.

Importing from an Existing Configuration Master

You can upgrade an existing configuration master to a new, higher configuration master version.

Step 1 On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.

Step 2 In the Options column, click **Import Configuration**.

Step 3 For **Select Configuration Source**, select a Configuration Master from the list.

- Step 4** Choose whether or not to include existing custom user roles in this configuration.
- Step 5** Click **Import**.

What to do next

[About Custom Web User Roles](#) , on page 410

Importing Settings from a Web Security Appliance

If you want to use an existing, working configuration from one of your Web Security appliances, you can import the configuration file to the Security Management appliance to create policy settings in a Configuration Master.

Before you begin

Verify compatibility of configuration files and Configuration Master versions. See [Determine the Configuration Master Versions to Use](#), on page 335.

**Caution**

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. 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.

**Note**

If you attempt to import a configuration file that uses an older set of the URL Categories than the Security Management appliance has, the load will fail.

-
- Step 1** Save a configuration file from the Web Security appliance.
- Step 2** On the Security Management appliance, choose **Web > Utilities > Configuration Masters**.
- Step 3** In the Options column, click **Import Configuration**.
- Step 4** From the Select Configuration drop-down list, select **Web Configuration File**.
- 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**.

Configuring Web Security Features Directly in Configuration Masters

You can configure the following functionality in a Configuration Master, depending on the version:

<ul style="list-style-type: none"> • Identities / Identification Profiles • SaaS Policies • Decryption Policies • Routing Policies • Access Policies • Web Traffic Tap Policies <p>Note To define Web Traffic Tap Policies, you must enable the Web Traffic Tap feature in the Web Security appliance.</p> <ul style="list-style-type: none"> • Overall Bandwidth Limits 	<ul style="list-style-type: none"> • Cisco Data Security • Outbound Malware Scanning • External Data Loss Prevention 	<ul style="list-style-type: none"> • SOCKS Policies • Custom URL Categories • Defined Time Ranges/ and Quotas • Bypass Settings • L4 Traffic Monitor
--	---	---

To configure settings for each feature directly in a configuration master, choose **Web > Configuration Master <version> > <feature>** .

Except for the few items described in [SMA-Specific Differences when Configuring Features in Configuration Masters](#), on page 342, instructions for configuring features in a Configuration Master are the same as instructions for configuring the same features on the Web Security appliance. For instructions, see the online help in your Web Security appliance or the AsyncOS for Cisco Web Security Appliances User Guide for the AsyncOS version corresponding to the Configuration Master version. If necessary, consult the following topic to determine the correct Configuration Master for your Web Security appliance: [Determine the Configuration Master Versions to Use](#), on page 335.

All versions of Web Security user guides are available from <https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html>.

SMA-Specific Differences when Configuring Features in Configuration Masters

When you configure a feature in a Configuration Master, note the following differences from configuring the same feature directly on the Web Security appliance.

Table 72: Feature Configuration: Differences between Configuration Master and Web Security Appliance

Feature or Page	Details
All features, especially new features in each release	For each feature that you configure in a Configuration Master, you must enable the feature in the Security Management appliance under Web > Utilities > Security Services Display. For more information, see Ensuring that Features are Enabled Consistently , on page 343.
Identities/Identification Profiles	<ul style="list-style-type: none"> • See Tip for Working with Identities/Identification Profiles in Configuration Masters, on page 343. • The Identify Users Transparently option when adding or editing an Identity/Identification Profile is available when a Web Security appliance with an authentication realm that supports transparent user identification has been added as a managed appliance.

Feature or Page	Details
Policies that use a Cisco Identity Services Engine (ISE) to identify users	<p>Secure Group Tag (SGT) information is updated from the Web Security appliances approximately every five minutes. The management appliance does not communicate directly with the ISE server.</p> <p>To update the list of SGTs on demand, select Web > Utilities > Web Appliance Status, click a Web Security appliance that is connected to the ISE server, then click Refresh Data. Repeat as needed for other appliances.</p> <p>The common deployment scenario is that a company has only one ISE server (this is the whole point of ISE) that all WSAs connect to. Multiple ISE servers with different data are not supported.</p>
Access Policies > Edit Group	<p>When you configure the Identities /Identification Profiles and Users option in the Policy Member Definition section, the following applies if you use external directory servers:</p> <p>When you search for groups on the Edit Group page, only the first 500 matching results are displayed. If you do not see the desired group, you can add it to the “Authorized Groups” list by entering it in the Directory search field and clicking the Add button.</p>
Access Policies > Web Reputation and Anti-Malware Settings	
SaaS Policies	The authentication option “Prompt SaaS users who have been discovered by transparent user identification” is available only when a Web Security appliance with an authentication realm that supports transparent user identification has been added as a managed appliance.

Tip for Working with Identities/Identification Profiles in Configuration Masters

When creating an Identity/Identification Profile 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/Identification Profiles for each appliance, then have policies which refer to those Identities/Identification Profiles. When the Security Management appliance publishes the configuration, those Identities/Identification Profiles 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/Identification Profile.

The only challenge with this method is if you have a default policy or Identity/Identification Profile 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/Identification Profiles and policies just above the default; essentially creating your own “default” policy.

Ensuring that Features are Enabled Consistently

Before you publish a Configuration Master, you should ensure that it will publish and that the intended features will be enabled and configured as you expect them to be after publishing.

To do this, do both of the following:

- [Comparing Enabled Features](#) , on page 344
- [Enabling Features to Publish](#) , on page 344



Note If multiple Web Security appliances with different features enabled are assigned to the same Configuration Master, you should publish to each appliance separately, and perform these procedures before each publish.

Comparing Enabled Features

Verify that the features enabled on each Web Security appliance match the features enabled for the Configuration Master associated with that appliance.



Note If multiple Web Security appliances with different features enabled are assigned to the same Configuration Master, you should publish to each appliance separately, and perform this check before each publish.

-
- Step 1** On the Security Management appliance, choose **Web > Utilities > Web Appliance Status**.
- Step 2** Click the name of a Web Security appliance to which you will publish a Configuration Master.
- Step 3** Scroll to the **Security Services** table.
- Step 4** Verify that the Feature Keys for all enabled features are active and not expired.
- Step 5** Compare the settings in the **Services** columns:
- The **Web Appliance Service** column and the **Is Service Displayed on Management Appliance?** column should be consistent.
- Enabled = Yes
 - Disabled and Not Configured = No or Disabled.
 - N/A = Not Applicable. For example, the option may not be configurable using a Configuration Master, but is listed so that you can see the Feature Key status.

Configuration mismatches will appear in red text.

What to do next

If the enabled/disabled settings for a feature do not match, do one of the following:

- Change the relevant setting for the Configuration Master. See [Enabling Features to Publish](#) , on page 344.
- Enable or disable the feature on the Web Security Appliance. Some changes may impact multiple features. See the information about the relevant feature in the AsyncOS for Cisco Web Security Appliances User Guide.

Enabling Features to Publish

Enable the features for which you want to publish settings using a Configuration Master.

Before you begin

Determine which features must be enabled and disabled. See [Comparing Enabled Features](#) , on page 344.

Step 1 On the Security Management appliance, choose **Web > Utilities > Security Services Display**.

Step 2 Click **Edit Settings**.

The Edit Security Services Display page lists the features that appear in each Configuration Master.

“N/A” alongside a feature indicates that the feature is not available in that Configuration Master version.

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) Hide Configuration Masters that you will not use. For instructions and cautions, see [Disabling Unused Configuration Masters](#) , on page 345 .

Step 4 For each Configuration Master that you will use, select or uncheck the Yes check box for each feature to enable.

Special notes for certain features (available options vary by Configuration Master version):

- Transparent Mode. If you use Forward mode, the proxy bypass feature will not be available.
- 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.

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 Commit your changes.

What to do next

- Verify that all features are now correctly enabled or disabled for the appliance to which you will publish. See [Comparing Enabled Features](#) , on page 344.
- On each Web Security appliance to which you will publish, make sure the features are enabled consistently with the features you have enabled for the Configuration Master.

Disabling Unused Configuration Masters

You can choose not to display unused Configuration Masters.

However, at least one Configuration Master must be enabled.



Note When a Configuration Master is disabled, 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.

-
- Step 1** On the Security Management appliance, choose **Web > Utilities > Security Services Display**.
- Step 2** Click **Edit Settings**.
- Step 3** Uncheck the checkbox(es) for unused Configuration Masters
- Step 4** Submit and commit your changes.
-

Setting Up to Use Advanced File Publishing

If your system is set up to use Configuration Masters, it is already set up for Advanced File Publishing.

Otherwise, complete procedures in the following topics, which apply to Advanced File Publishing as well as to publishing Configuration Masters.

- [Enabling Centralized Configuration Management on the Security Management Appliance](#), on page 335
- [Initializing Configuration Masters](#), on page 336
- [About Associating Web Security Appliances to Configuration Masters](#), on page 336

Publishing Configurations to Web Security Appliances

- [Publishing a Configuration Master](#), on page 346
- [Publishing Configurations Using Advanced File Publishing](#), on page 350

Publishing a Configuration Master

After editing or importing settings in a Configuration Master, you can publish them to the Web Security appliances associated with the Configuration Master.

- [Before You Publish a Configuration Master](#), on page 346
- [Publishing a Configuration Master Now](#), on page 348
- [Publishing a Configuration Master Later](#), on page 349
- [Publishing a Configuration Master Using the Command Line Interface](#), on page 349

Before You Publish a Configuration Master

Publishing a Configuration Master overwrites existing policy information on the Web Security appliances associated to that Configuration Master.

For information about which settings you can configure using a Configuration Master, see [Determining the Correct Configuration Publishing Method](#), on page 332.

All Publishing Jobs

- The AsyncOS version on the target Web Security appliance should be the same as the Configuration Master version, or be a version identified as compatible in the [SMA Compatibility Matrix](#).
- (First time only) You must follow the procedures in [Using Configuration Masters to Centrally Manage Web Security Appliances](#), on page 332.

- To ensure that the Configuration Master will publish and that the intended set of features will be enabled after publishing, verify the feature sets of each Web Security appliance and the associated Configuration Master and make any needed changes. See [Comparing Enabled Features , on page 344](#) and if necessary, [Enabling Features to Publish , on page 344](#). If you publish configurations for features that are not enabled on the target appliance, those configurations are not applied.

If different features are enabled on different Web Security appliances assigned to the same Configuration Master, you must publish to each appliance separately, and verify and enable features before each publish.

To identify configuration mismatches encountered during publishing, see [Viewing Publish History, on page 352](#) .

- Save a configuration file from each target Web Security appliance before publishing, so that you can restore the existing configuration in case of problems with the published configuration. See the AsyncOS for Cisco Web Security Appliances User Guide for details.
- Any change that would cause a Web proxy restart when committed on the Web Security appliance will also cause a proxy restart when you publish it from the Security Management appliance. You will receive a warning in these situations.

Web Proxy restarts temporarily interrupt web security services.

- When you publish any change to an Identity/Identification Profile, all end-users must re-authenticate.

Special Situations

- If you have reverted AsyncOS on the target Web Security appliance, you may need to associate a different Configuration Master with that appliance.
- If you publish a Configuration Master to a Web Security appliance that does not have a realm configured with Transparent User Identification enabled, but you have selected Transparent User Identification in an Identity /Identification Profile or SaaS Policy:
 - For Identities/Identification Profiles, Transparent User Identification is disabled and the Require Authentication option is selected instead.
 - For SaaS Policies, the Transparent User Identification option is disabled and the default option (Always prompt SaaS users for proxy authentication) is selected instead.
- When you publish External DLP policies from a Security Management appliance to multiple Web Security appliances that are not configured for RSA servers, the Security Management appliance will send the following publish status warning:

“The Security Services display settings configured for Configuration Master <version> 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 Names>”. 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.

If the Scheme in the Identity /Identification Profile in the Configuration Master Was:	Then the Scheme in the Identity /Identification Profile on the Web Security Appliance Becomes
Use Kerberos	Use NTLMSSP or Basic
Use Kerberos or NTLMSSP	Use NTLMSSP
Use Kerberos or NTLMSSP or Basic	Use NTLMSSP or Basic

If you are an externally authenticated user, you can only view the list of all the Configuration Master that are assigned to the Web Security appliance and publish the configuration that is currently initialized. If you want to publish a different subset of the Configuration Master, contact your administrator.



Note Do not edit, load, or publish Configuration Masters simultaneously using:

- Multiple tabs on the same browser.
- Multiple browsers on the same system or two different systems.

Publishing a Configuration Master Now

Before you begin

See important requirements and information in [Before You Publish a Configuration Master](#), on page 346.

Step 1 On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.

Step 2 Click **Publish Configuration Now**.

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.

Note If you configure a subset of a particular version of configuration master and assign a Web Security appliance, then the sub configuration master version that is associated to the Web Security appliance is displayed in the drop-down list.

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**.

Red progress bars and text on the Publish in Progress page 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.

What to do next

Check to be sure your publish was completely successful. See [Viewing Publish History, on page 352](#). Items that were not published completely will be noted.

Publishing a Configuration Master Later

Before you begin

See important requirements and information in [Before You Publish a Configuration Master , on page 346](#).

- Step 1** On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.
- Step 2** Click **Schedule a Job**.
- 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.
- 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.
- Step 9** You may want to create a reminder for yourself (for example, in your calendar) to check after the scheduled publish time to be sure that your publish was completely successful.

Note If you reboot or upgrade the appliance before the scheduled publishing job occurs, you must reschedule the job.

What to do next

Check to be sure your publish was completely successful. See [Viewing Publish History, on page 352](#). Items that were not published completely will be noted.

Publishing a Configuration Master Using the Command Line Interface



Note See important requirements and information in [Before You Publish a Configuration Master , on page 346](#).

The Security Management appliance provides you with the ability to publish changes through a Configuration Master using the following CLI command:

```
publishconfig config_master [--job_name ] [--host_list | host_ip ]
```

where **config_master** is a supported configuration master version. 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**.

Publishing Configurations Using Advanced File Publishing

Use advanced file publish to push a compatible XML configuration file from your local file system to managed Web Security appliances.

For information about which settings you can configure using Advanced File Publishing, see [Determining the Correct Configuration Publishing Method](#), on page 332.

To perform an advanced file publish:

- [Advanced File Publish: Publish Configuration Now](#), on page 350
- [Advanced File Publish: Publish Later](#), on page 351

Advanced File Publish: Publish Configuration Now

Before you begin

- Verify that the version of the configuration that you will publish is compatible with the AsyncOS version of the appliance to which you publish. See the Compatibility Matrix at <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>.
- On each destination Web Security appliance, back up the existing configuration on your Web Security appliance to a configuration file. See the AsyncOS for Cisco Web Security Appliances User Guide for details.

-
- Step 1** From the source Web Security appliance, save a Configuration File.
- For instructions on saving a configuration file from a Web Security appliance, see the AsyncOS for Cisco Web Security Appliances User Guide.
- Step 2** On the Security Management appliance window, choose **Web > Utilities > Publish to Web Appliances**.
- Step 3** Click **Publish Configuration Now**.
- Step 4** “System-generated job name” is selected by default, or enter a job name (up to 80 characters).
- Step 5** For **Configuration Master to Publish**, select **Advanced file options**.
- Step 6** Click **Browse** to select the file that you saved in Step 1.

- Step 7** 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 8** Click **Publish**.

Advanced File Publish: Publish Later

Before you begin

- Verify that the version of the configuration that you will publish is compatible with the AsyncOS version of the appliance to which you publish. See the Compatibility Matrix at <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>.
- On each destination Web Security appliance, back up the existing configuration on your Web Security appliance to a configuration file. See the AsyncOS for Cisco Web Security Appliances User Guide for details.

- Step 1** From the source Web Security appliance, save a Configuration File.
For instructions on saving a configuration file from a Web Security appliance, see the AsyncOS for Cisco Web Security Appliances User Guide.
- Step 2** On the Security Management appliance, choose **Web > Utilities > Publish to Web Appliances**.
- Step 3** Click **Schedule a Job**.
- Step 4** **System-generated job name** is selected by default, or enter a job name (up to 80 characters).
- Step 5** Enter the date and time when you want to publish the configuration.
- Step 6** For **Configuration Master to Publish**, select **Advanced file options**, then click **Browse** to select the configuration file that you saved in Step 1.
- Step 7** 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 8** Click **Publish**.

Viewing Status and History of Publishing Jobs

To View	Do This
A list of publishing jobs that are scheduled but have not yet occurred	Choose Web > Utilities > Publish to Web Appliances and look in the Pending Jobs section.
A list of the last published configuration per appliance	Choose Web > Utilities > Web Appliance Status and look at the Last Published Configuration information.
The status of a publishing job that is currently in progress	Choose Web > Utilities > Publish to Web Appliances and look in the Publishing Progress section.
History of all or any publishing jobs to all or any appliances	See Viewing Publish History

Viewing Publish History

Viewing the publish history is useful for checking for errors that may have occurred during publishing, or to identify mismatches between configured functionality and features enabled on target appliances.

-
- Step 1** On the Security Management appliance, choose **Web > Utilities > Publish History**.
- Step 2** To view additional details about a particular job, click the specific job name in the Job Name column.
- Step 3** View more information:
- To view status details about a particular appliance in the job, click a **Details** link.
- The Web Appliance Publish Details page appears.
- To view additional details about a particular appliance in the job, click the appliance name.
- The **Web > Utilities > Web Appliance Status** page appears.
-

Centralized Upgrade Management

You can simultaneously upgrade multiple Web Security appliances (WSAs) using a single Security Management Appliance (SMA). You also can apply a different software upgrade to each WSA.

- [Setting Up Centralized Upgrade Management for Web Security Appliances, on page 352](#)
- [Selecting and Downloading WSA Upgrades, on page 354](#)
- [Using the Install Wizard, on page 355](#)

Setting Up Centralized Upgrade Management for Web Security Appliances

Follow these steps to configure the Centralized Upgrade service on this Security Management Appliance:

- [Enable the Centralized Upgrade Manager, on page 352](#)
- [Adding the Centralized Upgrade Service to Each Managed Web Security Appliance, on page 353](#)

Enable the Centralized Upgrade Manager

Before you begin

- All Web Security appliances should be configured and working as expected before you enable centralized upgrade management.
- You must enable centralized upgrades individually on each managed Web Security appliance that will receive centralized upgrades.



Note To enable Centralized Upgrades in the CLI, use

```
applianceconfig > services > [...] > Enable Centralized Upgrade >
Y
```

- Be sure the appropriate feature key is installed on the Security Management Appliance.

-
- Step 1** On the Security Management appliance, select the **Management Appliance** page, and then choose **Centralized Services > Centralized Upgrade Manager**.
- Step 2** Click **Edit Settings**.
- Step 3** Check **Enable**.
- Step 4** Submit and commit your changes.
-

Adding the Centralized Upgrade Service to Each Managed Web Security Appliance

After enabling the Centralized Upgrade Manager on the Security Management appliance, you must add the desired Web Security appliance(s) to the Upgrade Manager roster by enabling Centralized Upgrades on the individual managed WSA(s).

-
- Step 1** On the Security Management appliance, select the **Management Appliance** page, and then choose **Centralized Services > Security Appliances**.
- Step 2** If you have not yet added Web Security appliances, or you need to add additional appliances for centralized upgrade management:
- Click **Add Web Appliance**.
 - In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Web Security appliance.
Note A DNS name may be entered in the IP Address text field, however, it will be resolved to an IP address when you click **Submit**.
 - Be sure to check **Centralized Upgrades**.
 - Click **Establish Connection**.
 - Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.
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.

Wait for the Success message to appear above the table on the page.
 - Click **Test Connection**.
Read test results above the table.
 - Click **Submit**.

Repeat this procedure for each WSA you want to add to the managed Web Security appliance list while simultaneously enabling Centralized Upgrade management.

- Step 3** To enable Centralized Upgrade management on a WSA already on this list of managed appliances:
- Click the name of the Web Security appliance to open its Edit Web Security Appliance Settings page.
 - Select **Centralized Upgrades** in the WSA Centralized Services section.
 - Click **Submit**.

Repeat this procedure for each WSA on which you want to enable Centralized Upgrade management.

- Step 4** Commit your changes.

What to do next

See [About Adding Managed Appliances, on page 19](#) for more information about adding to and editing the list of managed appliances.

Selecting and Downloading WSA Upgrades

- Step 1** On the Security Management appliance, select the **Web** page, and then choose **Utilities > Centralized Upgrade**. Any appliances recently selected for upgrade, and the upgrade status, are listed.
- Step 2** Click the **Upgrade Appliances** button on the Centralized Upgrade page. All managed WSAs which can be upgraded are listed.
- Step 3** Select each Web Security appliance to be upgraded by checking the box preceding its name in the list.
- Step 4** Click either **Download Wizard** or **Download and Install Wizard**.
- The Download Wizard lets you select upgrade packages for download to the selected WSA(s); this operation is download-only—you can install a downloaded package and restart each system later.
- The Download and Install Wizard lets you select upgrade packages for download and immediate installation on the selected WSA(s). After installation, each system is restarted automatically.
- Step 5** The Fetch Upgrades page of the launched wizard appears; when all available upgrades have been fetched for the selected WSAs (Completed Fetching Available Upgrades appears in the **Status** column of the WSA matrix), click **Next** to continue.
- Step 6** The Available Upgrades page lists all available upgrade builds for each selected WSA; select up to five for comparison, and then click **Next**.
- Step 7** The wizard's Upgrade Selection page presents a compatibility matrix of selected upgrades for each WSA; check the desired upgrade build for each WSA and then click **Next**.
- Step 8** The Summary page lists summary information for each selected WSA and upgrade build; click **Next** to continue the wizard.
- Step 9** Following a series of download checks such as WSA connection status, the Review page provides listings of download status for each WSA. Click **Begin Download** to begin downloading an upgrade package to each selected WSA.
- The Centralized Upgrade page displays download status information throughout the process.
-

What to do next

- **Download Wizard** – If you clicked this button at the beginning of this procedure, when download is complete, refresh the Centralized Upgrade page by choosing **Web > Utilities > Centralized Upgrade**, or by clicking the refresh-page button in your browser window.

In addition to the listing of all managed WSAs which can be upgraded, another section of the Centralized Upgrade page now lists all WSAs to which upgrade packages have been downloaded. (You can click the trash can button displayed with each entry to delete the downloaded upgrade package from that WSA.)

At any time you can select one or more WSAs in this list and then click Install Wizard to begin installation of the downloaded upgrade package on each selected WSA; when installation is complete on a WSA, it is restarted. See [Using the Install Wizard, on page 355](#) for information about using this wizard.

- **Download and Install Wizard** – If you clicked this button at the beginning of this procedure, when download is complete, upgrade installation begins automatically; see [Using the Install Wizard, on page 355](#), beginning with Step 2, for information about this process. When installation is complete, the WSA is restarted.

Using the Install Wizard

When the Install Wizard begins, whether automatically as part of the Download and Install process, or when you click the Install Wizard button on the Centralized Upgrade page after selecting one or more WSAs with downloaded but not-yet-installed upgrade packages, follow these step to configure installation.

-
- Step 1** If installing previously downloaded upgrade packages:
- a) Select the desired WSAs in the Web Appliances with Downloaded AsyncOS Versions section of the Centralized Upgrade page (**Web > Utilities > Centralized Upgrade**).
 - b) Click **Install Wizard**.
- Step 2** On the Upgrade Preparation page of the wizard, for each selected WSA:
- Check **Save the current configuration to the configuration directory before upgrading** if you want a back-up copy of the WSA's current configuration saved to that system's `configuration` directory.
 - If the **Save current configuration** option is checked, you can check **Mask passphrases in the configuration file** to have all current-configuration passphrases masked in the back-up copy. Note that the **Load Configuration** command cannot be used to reload back-up files with masked passphrases.
 - If the **Save current configuration** option is checked, you can enter one or more email addresses into the **Email file** to field; a copy of the back-up configuration file is mailed to each address. Separate multiple addresses with commas.
- Step 3** Click **Next**.
- Step 4** The Upgrade Summary page lists upgrade-preparation information for each selected WSA; click **Next** to continue the wizard.
- Step 5** Following a series of device checks such as connection status, the Review page provides a listing of installation status for each WSA. You can deselect devices that are showing an error. Click **Begin Install** to begin installing an upgrade package to each selected WSA.

You are returned to the Centralized Upgrade page where installation status information is displayed.

Note Each WSA will be restarted upon completion of the installation.

What to do next

Note Alternatively, you also can run the installer for any previously downloaded package from the WSA itself. That is, the downloaded upgrade package is listed on the WSA's **System Administration > System Upgrade** page, along with an Install button. See “Upgrading and Updating AsyncOS and Security Service Components” in the Cisco Web Security Appliances User Guide for more information.

Viewing Web Security Appliance Status

- [Comparing Enabled Features](#) , on page 344
- [Viewing a Summary of Status of Web Appliances](#) , on page 356
- [Viewing Status of Individual Web Security Appliances](#), on page 356
- [Web Appliance Status Details](#) , on page 357

Viewing a Summary of Status of Web Appliances

The **Web > Utilities > Web Appliance Status** page provides a high-level summary of the Web Security appliances connected to your Security Management appliance.

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. The warning icon indicates when attention is required for one of your connected appliances.

Viewing Status of Individual Web Security Appliances

The Appliance Status page provides a detailed view into the status of each connected appliance.

To view details for a managed Web Security appliance on the Web Appliance Status page, click the name of the appliance.

Status information includes general information about the connected Web Security appliances, their published configuration, publish history, feature key status, and so forth.



Note Only machines with support for centralized management will have data available for display.



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.

Web Appliance Status Details

Most of the information on this page is pulled from the Web Security appliance:

- 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)
- Centralized reporting status, including time of last attempted data transfer
- Status of features on Web Security appliances (whether each feature is enabled, status of feature keys)
- Acceptable Use Controls Engine versions on the managed and managing appliances
- AnyConnect Secure Mobility settings on the Web Security appliance
- Cisco Identity Services Engine (ISE) servers to which this Web Security appliance is connected.
- Proxy settings (upstream proxies and HTTP ports to proxy) for the Web Security appliance
- Authentication service information (servers, schemes, realms, and sequences; whether Transparent User Identification is supported; and whether to block or permit traffic if authentication fails)



Tip 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.

System Health Dashboard on the New Web Interface

On the appliance, choose **Monitoring > System Health** to monitor the system status. This page displays the current status and configuration of the Web Security appliance.



Note The System Health Dashboard with all critical and warning alerts is available in AsyncOS 14.0 releases and later only.

You can sort the page contents based on the time range -Date, Yesterday, Custom Range. While using Custom Range, the appliance enables you to select dates for a week.

The page displays the total number of web security appliance connected to the AsyncOS, the count of critical and warning alerts on appliances.

To search for a selected appliance, you must use the **search** feature.

To sort the appliances based in ascending and descending order, click the **Proxy Name**. However, you can only sort the rows only based on ascending and descending order of the **Proxy Name** field.



Note When your appliance has not established connected to Cisco Secure Manager, the row is highlighted and a stop icon appears when your hover your mouse over the row.

Details displayed include:

- Proxy Name- Displays the Web Security appliance proxy name.

- **Hardware**- Displays all hardware critical and warning alerts for the appliance. You must click on the alert to view a pop-up with information on the selected alert. To get detailed information about the alert, you must click on the **Hardware** link available on the pop-up. To navigate to the system status page of the selected appliance, select **Go To Appliance** link displayed in the pop-up. However, you must login to view the status page.
- **Services**- Displays all service critical and warning alerts for the appliance. You must click on the alert to view additional information on the selected alert. You must click on the alert to view a pop-up with information on the selected alert. To get detailed information about the alert, you must click on the **System** link available on the pop-up. To navigate to the system status page of the selected appliance, select **Go To Appliance** link displayed in the pop-up. However, you must login to view the status page.
- **Peak RPS**- Displays the number of requests per second for the selected appliance.
- **Peak Decrypted RPS**-Displays the peak RPS of decrypted requests on the appliance for the time period selected.
- **Peak Client Connections**- Displays the number of peak client-side connections on the appliance.
- **Peak Server Connections**- Displays the number of peak server-side connections on the appliance.

In AsyncOS 14.0, you can now view the current status and configuration of the Web Security appliance in a page. You must choose **Monitoring > System Health** to monitor the system status of the Web security appliances.

- In AsyncOS 14.1.0, the Web Security Appliance tracking data available on the interface is displayed based on the date the selected WSA was active. All status messages of the selected appliance is displayed based on the dates the appliance was available.
- AsyncOS 14.1.0 displays the Web Security Appliance status using color codes. The color codes used are:
 - Green status—API server and trailblazer are up and running
 - Grey status— Either API server status or and trailblazer status is either up and running or not. However, appliance connection is not established with Cisco Secure Email and Web Manager.
 - Red Status—Either API server status and trailblazer status is down or both are down.

Preparing For and Managing URL Category Set Updates

In order to ensure that your system has the latest set of predefined URL categories available for managing web usage, the URL category set for Web Usage Controls (WUC) may be updated occasionally: By default, Web Security appliances download URL category set updates automatically from Cisco, and the Security Management appliance receives these updates automatically within a few minutes from managed Web Security appliances.

Because these updates can impact existing configurations and appliance behavior, you should prepare in advance for these updates and take action after they occur.

Actions that you should take include the following:

- [Understand the Impacts of URL Category Set Updates , on page 359](#)
- [Ensure That You Will Receive Notifications and Alerts about URL Category Set Updates , on page 359](#)

- [Specify Default Settings for New and Changed Categories](#) , on page 359
- [When the URL Category Set is Updated, Check Your Policy and Identity/Identification Profile Settings](#) , on page 359

Understand the Impacts of URL Category Set Updates

When URL category set updates occur, they may change the behavior of existing policies in Configuration Masters.

For essential information about actions you should take before and after URL category set updates, see the “Managing Updates to the Set of URL Categories” section of the “URL Filters” chapter in the AsyncOS for Cisco Web Security Appliances User Guide at the link provided in [Documentation](#) , on page 629. Category descriptions are in the “URL Category Descriptions” section of the same chapter.

Ensure That You Will Receive Notifications and Alerts about URL Category Set Updates

To Receive	Do This
Advance notification of URL category set updates	Sign up now to receive notifications about your Cisco Secure Email and Web Manager appliances, which will include notifications about URL category set updates. See Cisco Notification Service , on page 629.
Alerts when URL category set updates have affected existing policy settings	Go to Management Appliance > System Administration > Alerts and make sure that you are configured to receive Warning-level alerts in the System category. More information about alerts is in Managing Alerts , on page 499.

Specify Default Settings for New and Changed Categories

Before URL category set updates occur, you should specify default actions for new and merged categories in each policy that offers URL filtering, or import a configuration from a Web Security appliance that has these settings already configured.

For more information, see the “Choosing Default Settings for New and Changed Categories” section in the “URL Filters” chapter of the AsyncOS for Cisco Web Security Appliances User Guide or the online help on the Web Security appliance.

When the URL Category Set is Updated, Check Your Policy and Identity/Identification Profile Settings

URL category set updates trigger two types of alerts:

- Alerts about category changes
- Alerts about policies that have changed or been disabled as a result of category changes

When you receive alerts about URL category set changes, you should check your existing URL category-based policies and Identities/Identification Profiles to be sure they still meet your policy goals.

For more information about the kinds of changes that might require your attention, see the “Responding to Alerts about URL Category Set Updates” section in the AsyncOS for Cisco Web Security Appliances User Guide.

Application Visibility and Control (AVC) Updates

The SMA automatically uses the version of the AVC engine that exists on the majority of the Web Security appliances that it manages.

Updating WBRs and AVC Data using CLI

You can use the `wsa_updatesconfig` command to update WBRs, AVC, or both WBRs and AVC data using CLI.

`wsa_updatesconfig`

Description

This command forces an update of WBRs, AVC, or both WBRs and AVC data on Secure Email and Web Manager. The following subcommands are available:

- WBRs - forces an update of WBRs data on Secure Email and Web Manager.
- AVC - forces an update of AVC data on Secure Email and Web Manager.
- BOTH - forces an update of WBRs and AVC data on Secure Email and Web Manager.

Usage

Commit: This command does not require a ‘commit.’

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

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

Example

```
mail1.example.com> wsa_updatesconfig
Choose the operation you want to perform:
- WBRs - force an update of WBRs data on this appliance.
- AVC - force an update of AVC data on this appliance.
- BOTH - force an update for WBRs and AVC on this appliance
```

Troubleshooting Configuration Management Issues

- [In Configuration Master Identities/Identification Profiles, Groups Are Not Available](#) , on page 361
- [Configuration Master Access Policies Web Reputation and Anti-Malware Settings Page Settings are Not as Expected](#), on page 361
- [Troubleshooting Configuration Publishing Failures](#) , on page 362

In Configuration Master Identities/Identification Profiles, Groups Are Not Available

Problem

In **Web > Configuration Master > Identities/Identification Profiles**, the Policy membership definition page doesn't show the Groups option under Selected groups and Users.

Solution

If you have multiple Web Security appliances: On each WSA, in **Network > Authentication**, make sure Realm Names are unique across all WSAs, unless all settings are identical for same-name realms.



Tip To see realm names for each WSA, go to **Web > Utilities > Web Appliance Status**, click each appliance name, and scroll to the bottom of the details page.

Configuration Master Access Policies Web Reputation and Anti-Malware Settings Page Settings are Not as Expected

Problem

The **Access Policies > Web Reputation and Anti-Malware Settings** page in the configuration master is missing expected settings, including the Web Reputation Score threshold settings and the ability to choose anti-malware scanning engines. Or it includes these settings when you are using Adaptive Security on the Web Security appliance.

Solution

Available options depend on whether Adaptive Security is selected for that configuration master in **Web > Utilities > Security Services Display** settings.

Troubleshooting Issues when Importing Existing Configuration for Configuration Masters

Problem

After you upgrade to Configuration Master 11.8, if you import an existing configuration to the new Configuration Master, the appliance redirects to the Web Security appliance (WSA_Sandbox) login page.

Solution

After you upgrade your appliance to a version supporting the Configuration Master 11.8, you must associate the Web Security appliances to the Security Management appliance to import configurations from an existing Configuration Master.



Note If you encounter any policy related issues when loading a configuration file, check for GUI logs on your appliance.

Troubleshooting Configuration Publishing Failures

Problem

Publishing a configuration fails.

Solution

Look at the **Web > Utilities > Web Appliance Status** page. Publishing fails if:

- There is a discrepancy between the status in the “Web Appliance Service” column and the status in the “Is Service Displayed on Management Appliance?” column.
- Both columns show that the feature is enabled but the corresponding Feature Key is not active (for example, is expired).
- The Configuration Master version should match the AsyncOS version on the Web Security appliance. Publishing an older Configuration Master version to a newer Web Security appliance may fail if settings on the Web Security appliance do not match the settings in the Configuration Master. This can occur even if the Web Appliance Status page does not indicate any discrepancies.

What to do Next:

- [Viewing Publish History, on page 352](#)
- [Comparing Enabled Features , on page 344](#)
- [Enabling Features to Publish , on page 344](#)



CHAPTER 12

Monitoring System Status

This chapter contains the following sections:

- [About Security Management Appliance Status](#), on page 363
- [Monitoring Service Status on the New Web Interface of the Appliance](#), on page 364
- [Monitoring Security Management Appliance Capacity](#), on page 365
- [Monitoring Status of Data Transfer From Managed Appliances](#), on page 366
- [Viewing the Configuration Status of Your Managed Appliances](#), on page 367
- [Monitoring Reporting Data Availability Status](#), on page 368
- [Monitoring Email Tracking Data Status](#), on page 369
- [Monitoring Capacity of Managed Appliances](#), on page 369
- [Identifying Active TCP/IP Services](#), on page 369
- [Replacing a Managed Appliance During Hardware Failure](#), on page 369

About Security Management Appliance Status

By default, the System Status page is the first page that appears when you access the Cisco Secure Email and Web Manager appliance from your browser. (To change the landing page, see [Setting Preferences](#), on page 543.)

To access the System Status page at any other time, select **Management Appliance > Centralized Services > System Status**.

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 centralized services, and added managed appliances, the Centralized Services section and the Security Appliance Data Transfer Status section are populated with data.

Status information includes the following:

- **Centralized Services:** Status of each centralized service, including Processing Queue usage
- **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 (operating system) version, build date, installation date, and serial number

Related Topics

- [Monitoring the Processing Queue](#) , on page 365
- [Monitoring CPU Utilization](#) , on page 365
- [Monitoring Status of Data Transfer From Managed Appliances](#) , on page 366

Monitoring Service Status on the New Web Interface of the Appliance

You can now monitor the status of your managed appliances and manage centralized services on the new web interface of your Secure Email and Web Manager appliance.

You can use the **Service Status** tab on the new web interface of your appliance to enable and disable centralized services such as email reporting, message tracking and quarantines.

The **Email Feature Status** section shows the services that are enabled and the number of licenses you have used for each service. Click **View Appliances** to view the number of added appliances. This redirects you to the legacy web interface of the appliance. For more information, see [About Adding Managed Appliances](#), on page 19

You can view the File Analysis details on the Service Status page of the new web interface of your appliance. You must join all managed appliances to the same appliance group in order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization.

You can enable and disable the following centralized services on the Service Status page:

- Centralized Reporting

For more information, see [Enabling Centralized Email Reporting on the New Web Interface](#), on page 51.

- Centralized Message Tracking

For more information, see [Enabling Centralized Email Tracking on the New Web Interface](#), on page 251.

- Centralized Spam Quarantines

For more information, see the following:

- [Enabling and Configuring Spam Quarantine on the New Web Interface](#), on page 270.
- [Notifying End Users About Quarantined Messages](#) , on page 292.
- [Configuring End-User Access to the Spam Quarantine](#) , on page 290.
- [Enabling Safelists and Blocklists on the New Web Interface](#), on page 278.

- Centralized Policy, Virus and Outbreak Quarantines

For more information, see [Enabling Centralized Policy, Virus, and Outbreak Quarantines on the New Web Interface of the Appliance](#) , on page 307.

- Safelists and Blocklists

For more information, see [Enabling Safelists and Blocklists on the New Web Interface](#), on page 278.

Monitoring Security Management Appliance Capacity

- [Monitoring the Processing Queue](#) , on page 365
- [Monitoring CPU Utilization](#) , on page 365

Monitoring the Processing Queue

You can periodically check the processing queue percentages used for email and web reporting and tracking to determine whether your appliance is running at optimal capacity.

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 managed appliances and processed by the Security Management appliance.



Note 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.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, select **Email** from the Product drop-down and choose **Service Status**.
- Step 2** On the Security Management appliance, choose **Management Appliance > Centralized Services > System Status**.
- Step 3** In the **Centralized Services** section at the top of the page, look at the Processing Queue percentages for:
- a) Centralized Reporting (Email Security subsection)
 - b) Centralized Message Tracking
 - c) Centralized Reporting (Web Security subsection)
- Step 4** If the processing queue usage percentages remain 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.
-

Monitoring CPU Utilization

To view the percentage of its CPU capacity that the Security Management appliance is using for each centralized service:

-
- Step 1** [New Web Interface Only] On the Security Management appliance, select **Email** from the Product drop-down and choose **Service Status**.
- Step 2** Select **Management Appliance > Centralized Services > System Status**.
- Step 3** Scroll to the **System Information** section and view the **CPU Utilization** subsection.

The CPU Utilization percentages indicate the portion of the Security Management appliance's CPU processing that is devoted to each of the main centralized services. Utilization percentages for some services may be combined. For example, email reporting are combined under "Reporting Service" while spam, policy, virus, and outbreak quarantines are combined under "Quarantine Services." Other operations of the Security Management appliance are grouped under the general heading "Security Management appliance."

Step 4 Refresh the browser display to view the most recent data.

The CPU utilization percentages change constantly.

Monitoring Status of Data Transfer From Managed Appliances

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 of the System Status page, you can view connection status issues for specific appliances. For detailed information about the status of each service on an appliance, click the appliance name to view the Data Transfer Status page for the appliance.

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.

Viewing the Configuration Status of Your Managed Appliances

You can view the configuration status of your managed appliances in one of the following ways:

- [New Web Interface Only] On the Security Management appliance, select **Email** from the Product drop-down and choose **Service Status**.
- On the Security Management appliance, choose **Management Appliance > Centralized Services > System Status**.

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.

Related Topics

- [Designating an Alternate Appliance to Process Released Messages, on page 310](#)
- [About Adding Managed Appliances, on page 19](#)

Additional Status Information for Web Security Appliances

For additional status information about Web Security appliances, see [Viewing Status of Individual Web Security Appliances, on page 356](#).

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 Email Security Reporting Data Availability, on page 368](#)

Monitoring Email Security Reporting Data Availability

To monitor reporting data from your Email Security appliances on the Security Management appliance, view the **Email > Reporting > Reporting Data Availability** page.

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.

Monitoring Web Security Reporting Data Availability

To monitor reporting data from your Web Security appliances on the Security Management appliance, view the **Web > Reporting > Data Availability** page.

From the Data Availability page you can update and sort data to provide real-time visibility into resource utilization and web traffic trouble spots.



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, on page 194](#) for more information on the Data Availability page on the Web Security appliance.

Monitoring Email Tracking Data Status

To monitor the status of email tracking data, view the **Email > Message Tracking > Message Tracking Data Availability** page.

Monitoring Capacity of Managed Appliances

You can monitor capacity of your managed appliances from the Security Management appliance. You can check the collective capacity of all Email or Web Security appliances and the capacity of each individual appliance.

To View Capacity of	See
Managed Web Security appliances	System Capacity Page, on page 192
Managed Email Security appliances	System Capacity Page, on page 91

Identifying Active TCP/IP Services

To identify active TCP/IP services used by your Security Management appliance, use the `tcpservices` command in the command line interface.

Replacing a Managed Appliance During Hardware Failure

If you have to replace a managed appliance due to a hardware failure or other reasons, the data from the replaced appliance will not be lost, but the data will not be displayed correctly on the Security Management appliance.

Upon replacing a managed appliance, add the new appliance to the list of hosts on the SMA, and connect it to the new appliance. If the IP address remains the same, change the IP on the old host entry to a non existing value.



CHAPTER 13

Integrating With LDAP

This chapter contains the following sections:

- [Overview, on page 371](#)
- [Configuring LDAP to Work with the Spam Quarantine, on page 371](#)
- [Creating the LDAP Server Profile, on page 372](#)
- [Configuring LDAP Queries, on page 374](#)
- [Domain-Based Queries, on page 378](#)
- [Chain Queries, on page 380](#)
- [Configuring AsyncOS to Work With Multiple LDAP Servers, on page 381](#)
- [Configuring External Authentication of Administrative Users Using LDAP , on page 384](#)

Overview

If you maintain end-user passphrases 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 the following users:

- End users and administrative users who access the spam quarantine.

When a user logs in to the web UI for the spam quarantine, the LDAP server validates the login name and passphrase, 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 spam quarantine, as long as the appliance does not rewrite them.

See [Configuring LDAP to Work with the Spam Quarantine, on page 371](#).

- Administrative users who sign in to the Cisco Secure Email and Web Manager appliance when External Authentication is enabled and configured.

See [Configuring External Authentication of Administrative Users Using LDAP , on page 384](#).

Configuring LDAP to Work with the Spam Quarantine

When you configure your Cisco Content Security 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, on page 372](#).

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, on page 381](#).

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, on page 374](#).

Step 3 Enable LDAP end-user access and spam notifications for the spam quarantine.

Enable LDAP end-user access to the 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 [Setting Up the Centralized Spam Quarantine](#).

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.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 Click **Add LDAP Server Profile**.

Step 4 Enter a name for the server profile in the **LDAP Server Profile Name** text field.

Step 5 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, on page 381](#).

Step 6 Select an authentication method. You can use anonymous authentication or specify a user name and passphrase.

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 Passphrase** radio button, and enter the User name and passphrase. The user name will now be seen on the User Mail Summary page.

Step 7 Select the LDAP server type: Active Directory, OpenLDAP, or Unknown or Other.

Step 8 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 9 Enter a base DN (distinguishing name) for the LDAP server.

If you authenticate with a user name and a passphrase, the user name must include the full DN to the entry that contains the passphrase. 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
```

- [Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings]: Check whether the Custom Certificate Authority is uploaded to validate the server certificate.
- To add the Certificate Authority, use `certconfig > CERTAUTHORITY` sub command in the CLI. [Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings and FQDN validation enabled in SSL Configuration settings]: Check whether the 'Common Name,' 'SAN: DNS Name' fields, or both present in the server certificate, are in the FQDN format.
- [Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings]: Check whether the 'Common Name,' or 'SAN: DNS Name' fields, of the server certificate contain Hostname of the server. Reverse DNS name is used if IP is configured in Hostname field.
- [Optional - Only if the 'Validate LDAP Server Certificate' is enabled in the LDAP Global Settings page and X 509 validation is enabled in the SSL Configuration settings page]: Check for the signature algorithm of the server certificate.
- [Optional - Only if the 'Validate LDAP Server Certificate' is enabled in the LDAP Global Settings page]: Check whether the server name is present in the 'Common Name' or 'SAN: DNS Name' fields in the server certificate.
- [Optional - Only if the 'Validate LDAP Server Certificate' is enabled in the LDAP Global Settings page]: Check the server certificate version.

Note Only version 1 and version 3 server certificates are allowed.

Step 10 Under Advanced, select whether to use SSL when communicating with the LDAP server.

Step 11 Enter the cache time-to-live. This value represents the amount of time to retain caches.

Step 12 Enter the maximum number of retained cache entries.

Step 13 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, on page 383](#).

Note The maximum number of simultaneous connections includes LDAP connections used for LDAP queries. However, if you enable LDAP authentication for the spam quarantine, the appliance allows 20 additional connections for the end user quarantine for a total of 30 connections.

Step 14 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, on page 374](#).

Step 15 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, on page 374](#).

Step 16 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 passphrases, the query can pass the test with an empty passphrase field.

Step 17 Submit and 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 spam quarantine query:

- **Spam quarantine end-user authentication query.** For more information, see the [Spam Quarantine End-User Authentication Queries, on page 375](#).
- **Spam quarantine alias consolidation query.** For more information, see [Spam Quarantine Alias Consolidation Queries, on page 377](#).

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, on page 378](#) and [Chain Queries, on page 380](#).



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, on page 375](#)
- [Tokens, on page 375](#)

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:
`((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, on page 378](#) for more information.

Spam Quarantine End-User Authentication Queries

End-user authentication queries validate users when they log in to the 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=smtp:{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 passphrase 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 73: Example LDAP Server and Spam Quarantine End-User Authentication Settings: Active Directory

Authentication Method	Use Passphrase (Need to create a low-privilege user to bind for searching, or configure anonymous searching.)
Server Type	Active Directory
Port	3268
Base DN	[Blank]
Connection Protocol	[Blank]
Query String	(sAMAccountName={u})
Email Attribute(s)	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 74: Example LDAP Server and Spam Quarantine End-User Authentication 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	[Blank]

Authentication Method	Anonymous
Query String	(uid={u})
Email Attribute(s)	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 (which may or may not be different for your deployment) 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 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, on page 377](#)
- [Sample OpenLDAP Alias Consolidation Settings, on page 378](#)

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 75: 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	((mail={a})(mail=smtp:{a}))
Email Attribute	mail

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 76: 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	(mail={a}))
Email Attribute	mail

Testing LDAP Queries

Use the Test Query button on the Add/Edit LDAP Server Profile page (or the `ldapttest` 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 `ldapttest` command is available as a batch command, for example:

```
ldapttest 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 Content Security 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 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, on page 372](#).
 - 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 spam quarantine. For more information about creating the query, see [Creating a Domain-Based Query, on page 379](#).
 - Step 3** Enable end-user access or spam notifications for the spam quarantine. For more information, see [Setting Up End-User Access to the Spam Quarantine via Web Browser, on page 289](#).
-

Creating a Domain-Based Query

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 On the LDAP page, click **Advanced**.

Step 4 Enter a name for the domain-based query.

Step 5 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 6 In the Domain Assignments field, enter a domain.







Step 7 Select a query to associate with the domain.

Step 8 Add a row and select a query for each domain in the domain-based query.

Step 9 Enter a default query to run if all other queries fail. If you do not want to enter a default query, select **None**.

Figure 6: Example Domain-based Query

Add Domain Assignments

Domain Assignments										
Name:	Bigfish_Auth									
Query Type:	Spam Quarantine End-User Authentication <input type="checkbox"/> Designate as the active query									
Domain Assignments:	<table border="1"> <thead> <tr> <th>Domain or Partial Domain</th> <th>Query</th> <th></th> </tr> </thead> <tbody> <tr> <td>bluefish.com</td> <td>Bluefish.isq_user_auth</td> <td></td> </tr> <tr> <td>redfish.com</td> <td>Redfish.isq_user_auth</td> <td></td> </tr> </tbody> </table>	Domain or Partial Domain	Query		bluefish.com	Bluefish.isq_user_auth		redfish.com	Redfish.isq_user_auth	
Domain or Partial Domain	Query									
bluefish.com	Bluefish.isq_user_auth									
redfish.com	Redfish.isq_user_auth									
Default Query:	None									
Test:	<input type="button" value="Test Query"/>									
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>										

Step 10 Test the query by clicking the Test Query button and entering a user login and passphrase or an email address to test in the Test Parameters fields. The results appear in the Connection Status field.

Step 11 Check the **Designate as the active query** checkbox if you want the 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 spam quarantine.

Step 12 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 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, on page 372](#).
- Step 2** Create the chain query and designate it as an active query for the spam quarantine. For more information, see [Creating a Chain Query, on page 380](#).
- Step 3** Enable LDAP end-user access or spam notifications for the spam quarantine. For more information about the spam quarantine, see [Setting Up the Centralized Spam Quarantine](#).

Creating a Chain Query



Tip You can also use the advanced subcommand of the `ldapconfig` command in the CLI.

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > LDAP > LDAP Server**.
- Step 3** From the LDAP Server Profiles page, click **Advanced**.
- Step 4** Click **Add Chained Query**.
- Step 5** Enter a name for the chain query.
- Step 6** 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 7 Select the first query in the chain.

The Cisco Content Security 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.

Figure 7: Example 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:	<table border="1"> <thead> <tr> <th>Order</th> <th>Query</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Server1.isq_user_auth</td> <td><input type="button" value="Add Row"/></td> </tr> <tr> <td>2</td> <td>Server2.isq_user_auth</td> <td><input type="button" value="Remove Row"/></td> </tr> </tbody> </table>	Order	Query		1	Server1.isq_user_auth	<input type="button" value="Add Row"/>	2	Server2.isq_user_auth	<input type="button" value="Remove Row"/>
Order	Query									
1	Server1.isq_user_auth	<input type="button" value="Add Row"/>								
2	Server2.isq_user_auth	<input type="button" value="Remove Row"/>								
Test:	Test_Query									

Step 8 Test the query by clicking the Test Query button and entering a user login and passphrase or an email address in the Test Parameters fields. The results appear in the Connection Status field.

Step 9 Check the **Designate as the active query** check box if you want the 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 spam quarantine.

Step 10 Submit and 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 Content Security 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 Content Security appliance to connect to redundant LDAP servers to use the following features:

- **Failover.** If the Cisco Content Security appliance cannot connect to an LDAP server, it connects to the next server in the list.
- **Load Balancing.** The Cisco Content Security 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. If the connection to the LDAP server fails, or the query returns an error for which it is appropriate to do so, the appliance attempts to query the next LDAP server specified in the list.


The Cisco Content Security 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, or the query returns an error, the appliance attempts to connect to the next LDAP server in the list. By default, the appliance always attempts to connect to the first server in the list, and it attempts to connect to each subsequent server in the order they are listed. To ensure that the Cisco Content Security appliance connects to the primary LDAP server by default, enter it as the first server in the list of LDAP servers.



Note Only attempts to query a specified LDAP server fail over. Attempts to query referral or continuation servers associated with the specified LDAP server do not fail over.

If the Cisco Content Security 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 Content Security Appliance for LDAP Failover

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > LDAP**.

Step 3 Select the LDAP server profile you want to edit.

In the following example, the LDAP server name is example.com.

Figure 8: Example LDAP Failover Configuration

LDAP Server Settings	
Server Attributes	
LDAP Server Profile Name:	example.com
Host Name(s):	ldapsrvr1.example.com, ldapsrvr2.example.com, ldapsrvr3.example.com <small>Fully qualified hostname or IP, separate multiple entries with a comma</small>
Authentication Method:	<input type="radio"/> Anonymous <input checked="" type="radio"/> Use Password Username: <input type="text"/> Password: <input type="password"/>
Server Type:	Unknown or Other
Port:	3268
Base DN:	dc=example, dc=com
Advanced:	
Connection Protocol:	<input type="checkbox"/> Use SSL
Cache TTL (time-to-live):	900 Seconds
Maximum Retained Cache Entries:	10000
Maximum number of simultaneous connections for each host:	10
Multiple host options:	<input type="radio"/> Load-balance connections among all hosts listed <input checked="" type="radio"/> Failover connections in the order listed

Step 4 In the Hostname text field, type the LDAP Servers; for example **ldapsrvr.example.com**.

Step 5 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 6** Click on the radio button next to **Failover connections in the order list**.
- Step 7** Configure other LDAP options as necessary.
- Step 8** Submit and 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 Content Security appliance distributes connections among the LDAP servers listed. If a connection fails or times out, the appliance determines which LDAP servers are available and reconnects to available servers. The appliance determines the number of simultaneous connections to establish based on the maximum number of connections you configure.

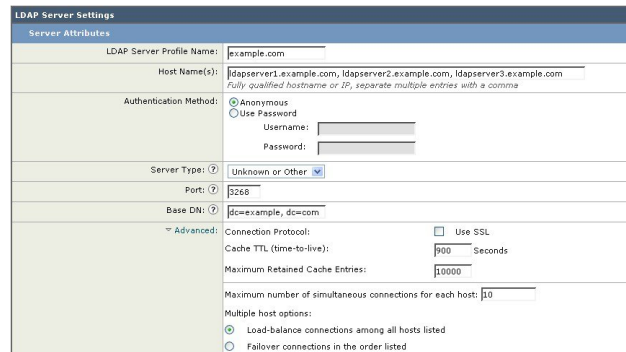
If one of the listed LDAP servers does not respond, the appliance distributes the connection load among the remaining LDAP servers.

Configuring the Cisco Content Security Appliance for Load Balancing

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > LDAP**.
- Step 3** Select the LDAP server profile you want to edit

In the following example, the LDAP server name is example.com.

Figure 9: Example Loadbalancing Configuration



LDAP Server Settings	
Server Attributes	
LDAP Server Profile Name:	example.com
Host Name(s):	ldapsrvr1.example.com, ldapsrvr2.example.com, ldapsrvr3.example.com <small>Fully qualified hostname or IP, separate multiple entries with a comma</small>
Authentication Method:	<input checked="" type="radio"/> Anonymous <input type="radio"/> Use Password Username: <input type="text"/> Password: <input type="password"/>
Server Type: ?	Unknown or Other
Port: ?	3268
Base DN: ?	dc=example, dc=com
Advanced:	Connection Protocol: <input type="checkbox"/> Use SSL Cache TTL (time-to-live): 900 Seconds Maximum Retained Cache Entries: 10000 Maximum number of simultaneous connections for each host: 10 Multiple host options: <input checked="" type="radio"/> Load-balance connections among all hosts listed <input type="radio"/> Failover connections in the order listed

- Step 4** In the Hostname text field, type the LDAP Servers; for example **ldapsrvr.example.com**.
- Step 5** 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 6** Click on the radio button next to **Load balance connections among all hosts**.
- Step 7** Configure other LDAP options as necessary.
- Step 8** Submit and commit the changes.

Configuring External Authentication of Administrative Users Using LDAP

You can configure the Cisco Content Security appliance to use an LDAP directory on your network to authenticate administrative users by allowing them to log in to the appliance with their LDAP user names and passphrases.

-
- Step 1** **Configure the LDAP Server Profile.** See [Creating the LDAP Server Profile, on page 372](#).
- Step 2** **Create a query to find user accounts.** In an LDAP server profile, in the External Authentication Queries section, create a query to search for user accounts in the LDAP directory. See [User Accounts Query for Authenticating Administrative Users, on page 384](#).
- Step 3** **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. For more information, see [Group Membership Queries for Authenticating Administrative Users, on page 385](#) and the documentation or online help for your Email Security appliance.
- Note** Use the **Test Queries** button in the External Authentication Queries section of the page (or the `ldapttest` command) to verify that your queries return the expected results. For related information, see [Testing LDAP Queries, on page 378](#).
- Step 4** **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 [Enabling External Authentication of Administrative Users, on page 386](#) and the “Adding Users” in the documentation or online help for your Email Security appliance.
-

User Accounts Query for Authenticating Administrative Users

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.

The following table shows the default query string and full user name attribute that AsyncOS uses when it searches for a user account on an Active Directory server.

Table 77: 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	(&(objectClass=user)(sAMAccountName={u}))
Attribute containing the user’s full name	displayName

The following table shows the default query string and full user name attribute that AsyncOS uses when it searches for a user account on an OpenLDAP server.

Table 78: 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 for Authenticating Administrative Users

You can associate LDAP groups with user roles for accessing the appliance.

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 user name, 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 user name 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 user names, you can use {dn} instead of {u}.

The following table shows the default query strings and attributes that AsyncOS uses when it searches for group membership information on an Active Directory server.

Table 79: Default Query String and Attributes for Active Directory Server

Query String	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})) Note If your LDAP schema uses distinguished names in the member of list instead of user names, you can replace {u} with {dn}

Query String	Active Directory
Query string to determine all members of a group	(&(objectClass=group)(cn={g}))
Attribute that holds each member's user name (or a DN for the user's record)	member
Attribute that contains the group name	cn


The following table shows the default query strings and attributes that AsyncOS uses when it searches for group membership information on an OpenLDAP server.

Table 80: Default Query String and Attributes for Open LDAP Server

Query String	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 user name (or a DN for the user's record)	memberUid
Attribute that contains the group name	cn

Enabling External Authentication of Administrative Users

After you configure the LDAP server profile and queries, you can enable external authentication using LDAP:

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 2** Choose **Management Appliance > System Administration > Users** page.
 - Step 3** Click **Enable**.
 - Step 4** Select the **Enable External Authentication** check box.
 - Step 5** Select **LDAP** for the authentication type.
 - Step 6** Select the LDAP external authentication query that authenticates users.
 - Step 7** Enter the number of seconds that the appliance waits for a response from the server before timing out.
 - Step 8** 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 9** Optionally, click **Add Row** to add another directory group. Repeat steps 7 and 8 for each directory group that the appliance authenticates.
 - Step 10** Submit and commit your changes.
-



CHAPTER 14

Configuring SMTP Routing

This chapter contains the following sections:

- [SMTP Routes Overview, on page 387](#)
- [Routing Email for Local Domains, on page 388](#)
- [Managing SMTP Routes , on page 389](#)

SMTP Routes Overview

This chapter explains the features that affect routing and delivery of email traveling through the Cisco Secure Email and Web Manager appliance, and use of the SMTP Routes page and `smtproutes` command.

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 operating system allows up to ten thousand (10,000) SMTP Route mappings to be configured for your Cisco Content Security appliance. (See [SMTP Routes Limits, on page 389](#).)

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.

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 Secure Email and Web Manager appliance sits behind a mail relay server that is at the edge of the network.

Routing Email for Local Domains

The Security Management appliance routes the following mail:

- ISQ released messages which ignore SMTP routing
- Alerts
- 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.

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.

Managing SMTP Routes

- [Defining an SMTP Route, on page 389](#)
- [SMTP Routes Limits, on page 389](#)
- [Adding SMTP Routes, on page 389](#)
- [Exporting SMTP Routes, on page 390](#)
- [Importing SMTP Routes, on page 390](#)
- [SMTP Routes and DNS, on page 391](#)

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 .

Adding SMTP Routes

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 2** Choose **Management Appliance > Network > SMTP Routes**.
 - Step 3** Click **Add Route**.
 - Step 4** 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 5** You can specify a port number by adding “:<port number> ” to the destination host: example.com:25
 - Step 6** Submit and commit your changes.
-

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.

- Step 1** Click **Export SMTP Routes** on the SMTP Routes page.
 - 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.

- Step 1** Click **Import SMTP Routes** on the SMTP Routes page.
- 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**.

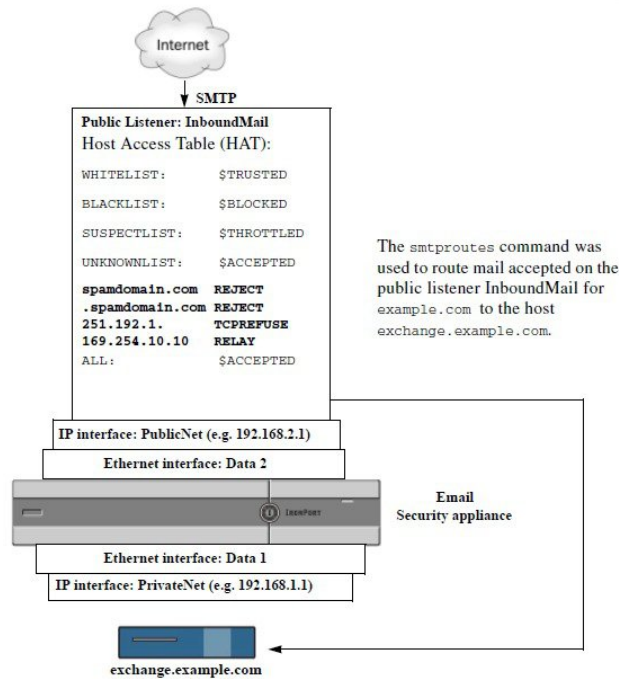
You can place “comments” in the file. Lines that begin with a ‘#’ character are considered comments and are ignored by AsyncOS. For example:

```
# this is a comment, but the next line is not
```

```
ALL:
```

At this point, our Email Gateway configuration looks like this:

Figure 10: Email Gateway Configuration



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
```




CHAPTER 15

Integrating with Cisco SecureX or Cisco Threat Response

This chapter contains the following topic:

[Integrating Your Appliance with Cisco SecureX or Cisco Threat Response , on page 393](#)

- [Integrating Your Appliance with Cisco SecureX or Cisco Threat Response , on page 393](#)

Integrating Your Appliance with Cisco SecureX or Cisco Threat Response

Cisco SecureX is a security platform embedded with every Cisco security product. It is cloud-native with no new technology to deploy. Cisco SecureX simplifies the demands of threat protection by providing a platform that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. By connecting technology in an integrated platform, Cisco SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. Cisco SecureX enables you to expand your capabilities by connecting your security infrastructure.

Cisco Cisco Threat Response is a threat incident response orchestration hub that supports and automates integrations across multiple Cisco Security products. As a key pillar of the Cisco integrated security architecture, Threat Response accelerates key security operations functions: detection, investigation, and remediation.

Integrating the Appliance with Cisco SecureX or Cisco Threat Response contains the following sections:

- [How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response , on page 394](#)
- [Performing Threat Analysis using Cisco SecureX Ribbon](#)

You can integrate your appliance with Cisco SecureX or Cisco Threat Response , and perform the following actions in Cisco SecureX or Cisco Threat Response :

- View and send the email data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in the email reports, sender and target relationships, search for multiple email addresses and subject lines and message tracking.
- Block compromised users or users violating outgoing email policies.

- Resolve the identified threats rapidly and provide recommended actions to take against the identified threats.
- Document the threats to save the investigation and enable collaboration of information among other devices.
- Block malicious domains, track suspicious observances, initiate an approval workflow or to create an IT ticket to update email policy.

You can access Cisco SecureX using the following URL:

<https://securex.us.security.cisco.com/login>

Cisco Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email security appliances. For more information on observables that can be enriched by the SMA Email module, go to <https://securex.us.security.cisco.com/settings/modules/available>, navigate to the module to integrate with Cisco SecureX , and click **Learn More**.

How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response

Table 81: How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites
Step 2	On your Security Management appliance, enable the Cisco SecureX or Cisco Threat Response integration.	Enable the Cisco SecureX Integration on your Security Management Appliance, on page 395
Step 3	On Cisco SecureX , add your appliance as a device, register it, and generate a registration token.	For more information, go to https://securex.us.security.cisco.com/help/settings-devices .
Step 4	On your Security Management appliance, complete the Cisco SecureX or Cisco Threat Response registration.	Register Cisco SecureX or Cisco Threat Response on Your Security Management Appliance, on page 396
Step 5	Confirm whether the registration was successful.	Confirm Whether the Registration was Successful
Step 6	On Cisco SecureX , add SMA Email Module.	For more information, go to https://securex.us.security.cisco.com/settings/modules/available , navigate to the module to integrate with Cisco SecureX , click Add New Module , and see the instructions on the page.

Prerequisites



Note If you already have a Cisco Threat Response user account, you do not need to create a Cisco SecureX user account. You can log in to Cisco SecureX using your Cisco Threat Response user account credentials.

- Make sure that you create a user account in Cisco SecureX with admin access rights. To create a new user account, go to **Cisco SecureX login** page using the URL <https://securex.us.security.cisco.com/login> and click **Create a SecureX Sign-on Account** on the login page. If you are unable to create a new user account, contact Cisco TAC for assistance.
- [Only if you are not using a proxy server] Make sure that you open HTTPS (In and Out) 443 port on the firewall for the following FQDNs to register your appliance with Cisco SecureX or Cisco Threat Response :
 - api-sse.cisco.com (applicable for NAM users only)
 - api.eu.sse.itd.cisco.com (applicable for European Union (EU) users only)
 - api.apj.sse.itd.cisco.com (applicable for APJC users only)
 - est.sco.cisco.com (applicable for APJC, EU, and NAM users)

For more information, see [Firewall Information, on page 621](#).

Enable the Cisco SecureX Integration on your Security Management Appliance

-
- Step 1** Log in to your appliance.
- Step 2** Select **Networks > Cloud Service Settings**.
- Step 3** Click **Edit Global Settings**.
- Step 4** Check the **Enable** check box.
- Step 5** Submit and commit your changes.
- Step 6** Wait for few minutes, and check whether the **Register** button appears on your appliance.
-



Note In a clustered configuration, you can only register your logged-in appliance with Cisco SecureX or Cisco Threat Response in the machine mode. If you have already registered your appliance with Cisco SecureX or Cisco Threat Response in the standalone mode, make sure to deregister the appliance manually before you join it to a cluster.



Note To enable this integration using the CLI, use the `threatresponseconfig` command.

What to do next

Register your appliance on Cisco SecureX or Cisco Threat Response . For more information, go to <https://securex.us.security.cisco.com/settings/modules/available>, navigate to the module to integrate with Cisco SecureX, click **Get Started**, and see the instructions on the page.

Register Cisco SecureX or Cisco Threat Response on Your Security Management Appliance

- Step 1** Go to **Networks > Cloud Service Settings**.
- Step 2** In **Cloud Services Settings**, enter the registration token, and click **Register**.
-



Note To register Cisco SecureX or Cisco Threat Response using the CLI, use the `cloudserviceconfig` command.

What to do next

[Confirm Whether the Registration was Successful](#)

Reregistering with Cisco Cloud Service Portal

You can reregister your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal based on any one of the following scenarios:

- If you are unable to view or manage the devices (Cisco Secure Email and Web Managers) added to the Cisco Cloud Services portal when you automatically register your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.
- If your Smart Account and Cisco Cloud Services Account are not linked when you automatically register your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.

You can also use the `cloudserviceconfig > reregister` sub command in the CLI to reregister your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.

Before you begin

Make sure you have met the following prerequisites:

- Enabled Smart Software Licensing on your Cisco Secure Email and Web Manager.
 - Registered your Cisco Secure Email and Web Manager with Cisco Smart Software Manager.
-

- Step 1** Go to **Networks > Cloud Service Settings** page on your Cisco Secure Email and Web Manager.
- Step 2** Click **Reregister**.

Note After you click Reregister, you can choose whether you want to perform the task in either steps 3 or 4 or both depending on your requirement.

- Step 3** [Optional] Choose the appropriate Cisco Secure Server to connect your Cisco Secure Email and Web Manager to the Cisco Cloud Services portal if your device was automatically registered with an incorrect Cisco Secure server.

- Step 4** [Optional] Enter the registration token obtained from the Cisco Cloud Services portal, if your Cisco Secure Email and Web Manager was automatically registered with an incorrect Smart Account.
- Step 5** Click **Submit**, the 'Confirm reregistration' dialog box appears only if you do not enter a registration token in step 4.
- Step 6** Click **Submit**, in the 'Confirm reregistration' dialog box to allow Cisco Cloud Services to use the token auto-generated from the Cisco Cloud Services portal with the Smart Account information to reregister your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.
-

Confirm Whether the Registration was Successful

- On security services exchange, confirm successful registration by reviewing the status in security services exchange.
- On Cisco SecureX , navigate to the **On-Premises Appliances** page (<https://xdr.us.security.cisco.com/administration/on-premise-appliances>) and view the SMA that has been registered with security services exchange.



Note

If you want to switch to another Cisco SecureX or Cisco Threat Response server (for example, 'Europe - api.eu.sse.itd.cisco.com'), you must first deregister your appliance from Cisco SecureX or Cisco Threat Response and follow steps mentioned in [How to Integrate Your Appliance with Cisco SecureX or Cisco Threat Response](#) , on page 394.

After you have integrated your appliance with Cisco SecureX or Cisco Threat Response , you do not need to integrate your Email Security appliance with Cisco SecureX or Cisco Threat Response because the email and web reporting features are centralized.

After successful registration of your appliance on security services exchange, add the SMA Email module on Cisco SecureX . For more information, go to <https://securex.us.security.cisco.com/settings/modules/available>, navigate to the module to integrate with Cisco SecureX , and click **Add New Module**, and see the instructions on the page.

Enabling Cisco SecureX or Threat Response on content Security Gateway

- Step 1** Log in to your appliance.
- Step 2** Select **Networks > Cloud Service Settings**.
- Step 3** Click **Enable**.
- Step 4** Check the **Enable Cloud Service** check box.
- Step 5** Choose the Cisco SecureX server.
- Step 6** Submit and commit your changes.
-

Enabling Cisco Cloud Services Portal on Content Security Gateway

- Step 1** Log in to your email gateway.
 - Step 2** Select **Networks > Cloud Service Settings**.
 - Step 3** Click **Enable**.
 - Step 4** Check the **Enable Cisco Cloud Services** check box.
 - Step 5** Choose the required Cisco Secure server to connect your email gateway to the Cisco Cloud Services portal.
 - Step 6** Submit and commit your changes. Wait for few minutes, and check whether the Register button appears on your content security gateway.
-

What to do next

Performing Threat Analysis using Cisco SecureX Ribbon



Note When you upgrade from Security Management Appliance 13.6.1 or earlier versions, **Casebook** will be part of the Cisco SecureX Ribbon.

Cisco SecureX supports a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting. These distributed capabilities are presented in the form of applications (apps) and tools in the Cisco SecureX Ribbon.

This topic contains the following sections:

- [Accessing the Cisco SecureX Ribbon](#)
- [Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu](#)

You will find the Cisco SecureX Ribbon at the bottom pane of the page, and it persists as you move between the dashboard and other security products in your environment. Cisco SecureX Ribbon consists of the following icons and elements:

- Expand/Collapse Ribbon
- Home
- Casebook App
- Incidents App
- Orbital App
- Enrichment Search Box
- Find Observables
- Settings

For more information on Cisco SecureX Ribbon, see <https://securex.us.security.cisco.com/help/ribbon>.


Accessing the Cisco SecureX Ribbon

Before you begin

Make sure that you meet all the prerequisites that are mentioned in [Prerequisites](#).



Note Suppose you have already configured **Casebook** for Security Management Appliance 13.6.1 or earlier versions, you need to create a **Client ID** and **Client Secret** in Cisco SecureX API client with additional scopes, as mentioned in the following procedure.

You can drag the Cisco SecureX Ribbon, positioned at the bottom pane of the page, from right using  button.

- Step 1** Log in to the new web interface of your appliance. For more information, see [Accessing the Web Interface](#).
- Step 2** Click the Cisco SecureX Ribbon.
- Step 3** Create a **Client ID** and **Client Secret** in **SecureX API Clients**. For more information to generate API Client credentials, see [Creating an API Client](#).

While creating a client ID and client password, make sure that you choose the following scopes:

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (if you have access)

- Step 4** Enter the client ID and client password obtained in [Step 3](#) in the **Login to use SecureX Ribbon** dialog box in your appliance.
- Step 5** Select the required Cisco SecureX server in the **Login to use SecureX Ribbon** dialog box.
- Step 6** Click **Authenticate**.

Note If you want to edit the client ID, client password, and Cisco SecureX server, right-click on the Cisco SecureX Ribbon, and add the details.

What to do next


[Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu](#)

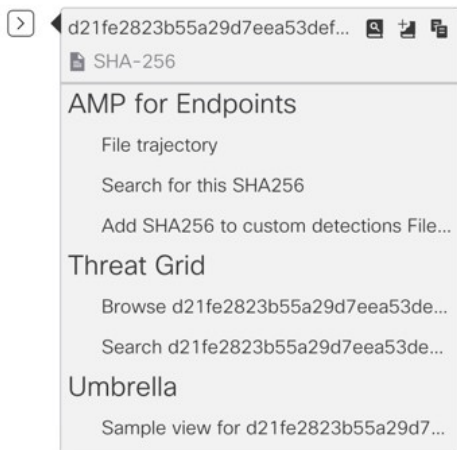
Adding Observable to Casebook for Threat Analysis using Cisco SecureX Ribbon and Pivot Menu

Before you begin



Make sure that you obtain the client ID and client password to access the Cisco SecureX Ribbon and pivot menu widgets on your appliance. For more information, see [Accessing the Cisco SecureX Ribbon](#).

Step 1 Log in to the new web interface of your appliance. For more information, see [Accessing the Web Interface](#).


Step 2 Navigate to the **Email Reporting** or **Web Reporting** page, click the pivot menu  button next to the required observable (for example, bit.ly).






Perform the following:

- Click  button to add an observable to active case.
- Click  button to add the observable to new case.

Note


Use the pivot menu  button to pivot an observable to other devices registered on the portal (for example, AMP for Endpoints) to investigate for threat analysis.

Step 3 Hover over  icon and click  button to open the **Casebook**. Check whether the observable is added to a new or an existing case.

Step 4 (Optional) Click  button to add a title, description, or notes to the **Casebook**.



Note You can search for observables for threat analysis in two different ways:

- Click the **Enrichment**  search box from the Cisco SecureX Ribbon and search for the observables.
- Click the **Casebook** icon inside the Cisco SecureX Ribbon and search for the observables in the search



field.

For more information on Cisco SecureX Ribbon, see <https://securex.us.security.cisco.com/help/ribbon>.

Performing Remedial Actions on Messages in Cisco SecureX Threat Response

Before you begin

In Cisco Threat Response , you can now investigate and apply the following remedial actions on messages processed by your Secure Email and Web Manager:

- Delete
- Forward
- Forward and Delete

Make sure you have met the following prerequisites before you perform remedial actions on messages in Cisco Threat Response :

- Enabled and registered your Secure Email and Web Manager with the Cisco SecureX server. For more information, see [Enable the Cisco SecureX or Cisco Threat Response Integration on your Cisco Content Security Appliance and Registering Cisco SecureX or Cisco Threat Response on Cisco Content Security Appliance](#) .
- Added your Secure Email and Web Manager module to Cisco SecureX and specified the Remediation Forwarding Address in Cisco SecureX . For more information, go to <https://securex.us.security.cisco.com/settings/modules/available> navigate to the required Secure Email and Web Manager module to integrate with Cisco SecureX , click Add New Module, and see the instructions on the page.
- Enabled and configured the remediation profiles in the **System Administration > Account Settings** page in your email gateway. For more information, see the Remediating Messages in Mailboxes chapter of the Cisco Secure Email Gateway User Guide.

Step 1 Log in to Cisco SecureX with your user credentials.

Step 2 Perform an investigation for threat analysis by entering required IOCs (for example, URLs, Email Message ID and so on) in the Investigate panel and click Investigate. For more information, see the Investigate topic in the Help section at <https://visibility.amp.cisco.com/help/investigate>.

- Step 3** Click the pivot menu button next to the Cisco Message ID or Email Message ID and select the required remedial action (for example, 'Forward'). For more information, see the Pivot Menu topic in the Help section at <https://visibility.amp.cisco.com/help/investigate>.
-



CHAPTER 16

Distributing Administrative Tasks

This chapter contains the following sections:

- [About Distributing Administrative Tasks](#) , on page 403
- [Assigning User Roles](#) , on page 403
- [Users Page](#) , on page 412
- [About Authenticating Administrative Users](#), on page 413
- [Additional Controls on Access to the Security Management Appliance](#), on page 426
- [Controlling Access to Sensitive Information in Message Tracking](#) , on page 430
- [Displaying a Message for Administrative Users](#), on page 431
- [Enabling and Disabling Message Banners for Administrative Users](#), on page 431
- [Viewing Administrative User Activity](#) , on page 431
- [Troubleshooting Administrative User Access](#) , on page 433

About Distributing Administrative Tasks

You can distribute administrative tasks on the Cisco Content Security Management appliance to other people based on the user roles that you assign to their user accounts.

To set up to distribute administrative tasks, you will determine whether the predefined user roles meet your needs, create any needed custom user roles, and set up the appliance to authenticate administrative users locally on the security appliance, and/or externally using your own centralized LDAP or RADIUS system.

Additionally, you can specify additional controls on access to the appliance and to certain information on the appliance.

Assigning User Roles

- [Predefined User Roles](#) , on page 404
- [Custom User Roles](#) , on page 406

Additional configuration is required for quarantine access. See [Access to Quarantines](#) , on page 412.

Predefined 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 82: Descriptions of User Roles

User Role Name	Description	Web Reporting/Scheduled Reports Capability
admin	<p>The admin 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 passphrase.</p> <p>Only the admin user can issue the resetconfig and revert commands.</p>	Yes/Yes
Administrator	User accounts with the Administrator role have full access to all configuration settings of the system.	Yes/Yes
Operator	<p>User accounts with the Operator role are restricted from:</p> <ul style="list-style-type: none"> • Creating or editing user accounts • Upgrading the appliance • Issuing the <code>resetconfig</code> command • Running the System Setup Wizard • Modifying LDAP server profile settings other than username and passphrase, if LDAP is enabled for external authentication. • Configuring, editing, deleting, or centralizing quarantines. <p>Otherwise, they have the same privileges as the Administrator role.</p>	Yes/Yes
Technician	User accounts with the Technician role can initiate system administration activities such as upgrades and reboots, save a configuration file from the appliance, manage feature keys, and so forth.	Access to System Capacity reports under the Web and Email tabs

User Role Name	Description	Web Reporting/Scheduled Reports Capability
Read-Only Operator	<p>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 most changes to see how to configure a feature, but they cannot commit them or make any change that does not require a commit. Users with this role can manage messages in quarantines, if access is enabled.</p> <p>Users with this role cannot access the following:</p> <ul style="list-style-type: none"> • File system, FTP, or SCP. • Settings for creating, editing, deleting or centralizing quarantines. 	Yes/No
Guest	<p>Users accounts with the Guest role can view status information including reports and Web Tracking, and manage messages in quarantines, if access is enabled. Users with the Guest role cannot access Message Tracking.</p>	Yes/No
Web Administrator	<p>User accounts with the Web Administrator role have access to all configuration settings under the Web tab.</p>	Yes/Yes
Web Policy Administrator	<p>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.</p>	No/No
Email Administrator	<p>User accounts with the Email Administrator role have access to all configuration settings within the Email menu only, including quarantines.</p>	No/No
Help Desk User	<p>User accounts with the Help Desk User role are restricted to:</p> <ul style="list-style-type: none"> • Message Tracking • Managing messages in quarantines <p>Users with this role cannot access the rest of the system, including the CLI. After you assign a user this role, you must also configure quarantines to allow access by this user.</p>	No/No

User Role Name	Description	Web Reporting/Scheduled Reports Capability
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>These features can be access log subscriptions, Logging APIs, and log files.</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 > System Administration > User Roles and click the user name.</p> <p>Note Users assigned to a Custom Email User Role cannot access the CLI.</p> <p>For more information, see Custom User Roles , on page 406.</p>	No/No

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.

Administrators can create custom roles with read-only option for Quarantine messages. The read-only option prevents users from deleting or releasing messages and only have read-only access to quarantine.

For more information, see:

- [About Custom Email User Roles , on page 406](#)
- [Deleting Custom User Roles , on page 412](#)

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)
- AMP Reports (optionally restricted by Reporting Group)
- Message Tracking
- Quarantines
- Log Subscription

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 Custom user roles on the Email Security appliance offer more granular access than do 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 documentation or online help for your Email Security appliance.

Access to 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 Security Reporting, on page 49](#).

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:

- Mail Flow Summary
- Mail FLOW Details
- Outgoing Destinations
- User Mail Summary
- DLP Incidents
- Content Filters
- Virus Filtering
- TLS Encryption
- 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:

- Mail Flow Summary
- Mail Flow Details
- Outgoing Destinations
- User Mail Summary
- Content Filters
- Virus Filtering
- 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
- Archived Reports

AMP Reports

If you grant a custom role access to AMP Reports, users assigned to this role can view the following AMP-related reports for all email gateways or the selected Reporting Group:

- Advanced Malware Protection (AMP Reputation)
- File Analysis
- AMP Verdict Update (File Retrospection)
- Mailbox Auto Remediation

Access to Message Tracking Data

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 [Controlling Access to Sensitive Information in Message Tracking](#), on page 430.

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 Messages](#), on page 249.

Access to Quarantines for Custom User Role

If you grant a custom role access to quarantines, users to whom you assign this role can search for, view, release, or delete messages in all quarantines on this Security Management appliance.

Before users can access quarantines, you must enable that access. See [Access to Quarantines](#), on page 412.

Log Subscription

The Log Subscription access privileges define whether delegated administrators assigned to the custom user role can access log subscriptions or Logging APIs to view or download log files.


Creating Custom Email User Roles

You can create custom email user roles for access to Email Reporting, Message Tracking, and quarantines.

For descriptions of the access that each of these options permits, see [About Custom Email User Roles](#), on page 406 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 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > User Roles**.

Step 3 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.

Step 4 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.
- The name must contain only lowercase letters, numbers, and dashes. It cannot start with a dash or a number.
- If you grant users with this role access to centralized policy quarantines, and you also want users with this role to be able to specify those centralized quarantines in message and content filters and DLP Message Actions on an Email Security appliance, the name of the custom role must be the same on both appliances.

Step 5 Choose the access privileges to enable for this role.

Administrators can create custom roles with read-only option for Quarantine messages. The read-only option prevents users from deleting or releasing messages and only have read-only access to quarantine.

Step 6 Click **Submit** to return to the User Roles page, which lists the new user role.

Step 7 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 8 Commit your changes.

Step 9 If you granted this role access to quarantines, enable access for this role:

See:

- [Configuring Administrative User Access to the Spam Quarantine](#), on page 274
 - [Configuring Policy, Virus, and Outbreak Quarantines](#), on page 314
-

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 11: 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	Mail Policy Reports from all Email Appliances <i>View and analyze email traffic.</i>
Message Tracking	Message Tracking <i>Track messages.</i>
Quarantines	Manage messages in the Spam Quarantine <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 a 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, on page 411](#)
- [Editing Custom Web User Roles, on page 411](#)
- [Deleting Custom User Roles, on page 412](#)

Creating Custom Web User Roles

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > User Roles**.
- Step 3** 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.
- Step 4** 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 5** Choose whether you want the policies and custom URL categories to be visible or hidden by default.
- Step 6** 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 7** 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 8** 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 [Scheduling Web Reports](#), on page 221 section in chapter [Using Centralized Web Reporting and Tracking](#), on page 163. 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.
- 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

- 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.

Deleting Custom User Roles

If you delete a custom user role that is assigned to one or more users, you do not receive an error.

User Roles with Access to the CLI

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 (for web security), and custom user.

Using LDAP

If you use an LDAP directory to authenticate users, you assign directory groups to user roles instead of to 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 User Authentication](#) , on page 421.

Access to Quarantines

Before users can access quarantines, you must enable that access. See the following information:

- [Configuring Administrative User Access to the Spam Quarantine](#) , on page 274
- [About Distributing Message Processing Tasks to Other Users](#) , on page 320 (for policy quarantines), and [Configuring Policy, Virus, and Outbreak Quarantines](#) , on page 314
- [Configuring Centralized Quarantine Access for Custom User Roles](#)

Users Page

For Information About This Section	See
Users	About Distributing Administrative Tasks , on page 403
Reset Passphrases button	Managing Locally-Defined Administrative Users , on page 414 Requiring Users to Change Passphrase on Demand , on page 420
Local User Account & Passphrase Settings	Setting Passphrase and Login Requirements , on page 416
External Authentication	External User Authentication , on page 421
DLP Tracking Privileges	Controlling Access to Sensitive Information in Message Tracking , on page 430

About Authenticating Administrative Users

You can control access to the appliance by defining authorized users locally on the appliance, and/or by using external authentication or two-factor authentication.

- [Changing the Admin User’s Passphrase, on page 413](#)
- [Changing the User’s Passphrase After Expiry, on page 413](#)
- [Managing Locally-Defined Administrative Users , on page 414](#)
- [External User Authentication , on page 421](#)
- [Two-Factor Authentication, on page 424](#)


Changing the Admin User’s Passphrase

Any administrator-level user can change the passphrase for the “admin” user, via the GUI or the CLI.



Note Cisco recommends you to change the passphrase when you log in to the appliance for the first time or if you reset the configurations to factory defaults.

To change the passphrase via the GUI, do the following:

- [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Choose **Management Appliance > System Administration > Users** page and select the admin user.

To change the passphrase for the admin user in the CLI, use the `passphrase` command. The `passphrase` command requires you to enter the old passphrase for security.

If you forget the passphrase for the “admin” user account, contact your customer support provider to reset the passphrase.



Note Changes to the passphrase take effect immediately and do not require you to commit the change.

Changing the User’s Passphrase After Expiry

If your account has expired, you will be prompted with the following message “Your passphrase expired. Please change your passphrase by clicking here.”

Click on the link and enter the login details with your expired passphrase, to proceed to the Change Passphrase page. For more information on setting passphrases, [Setting Passphrase and Login Requirements , on page 416](#).



Note Changes to the passphrase take effect immediately and do not require you to commit the change.

Managing Locally-Defined Administrative Users

- [Adding Locally-Defined Users, on page 414](#)
- [Editing Locally-Defined Users, on page 415](#)
- [Deleting Locally-Defined Users, on page 415](#)
- [Viewing the List of Locally-Defined Users , on page 415](#)
- [Setting and Changing Passphrases , on page 415](#)
- [Setting Passphrase and Login Requirements , on page 416](#)
- [Requiring Users to Change Passphrase on Demand , on page 420](#)
- [Locking and Unlocking Local User Accounts , on page 420](#)


Adding Locally-Defined Users

Follow this procedure to add users directly to the Security Management appliance if you are not using external authentication. Alternatively, use the `userconfig` command in the CLI.



Note If external authentication is also enabled, be sure that local user names do not duplicate externally-authenticated user names.

There is no limit to the number of user accounts that you can create on the appliance.

-
- Step 1** If you will assign custom user roles, we recommend that you define those roles first. See [Custom User Roles , on page 406](#).
- Step 2** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 3** Choose **Management Appliance > System Administration > Users**.
- Step 4** Click **Add User**.
- Step 5** Enter a unique name for the user. You cannot enter words that are reserved by the system (such as “operator” and “root”).
- If you also use external authentication, user names should not duplicate externally-authenticated user names.
- Step 6** Enter a full name for the user.
- Step 7** Select a predefined role or a custom role. See the table *Descriptions of User Roles* in section [Predefined User Roles , on page 404](#) 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 , on page 409](#) or [Creating Custom Web User Roles, on page 411](#).
- Step 8** Confirm your current passphrase for security validation.
- Step 9** You can generate or enter a passphrase and re-enter the passphrase to confirm the same.
- Step 10** Submit and commit your changes.

Step 11 If you added a custom user role on this page, assign privileges to that role now. See [Custom User Roles](#) , on page 406.

Editing Locally-Defined Users

Use this procedure to change a passphrase, for example.

- Step 1** Click the user's name in the Users listing.
 - Step 2** Make changes to the user.
 - Step 3** Confirm your current passphrase for security validation.
 - Step 4** Submit and commit your changes.
-

Deleting Locally-Defined Users

- 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.
-

Viewing the List of Locally-Defined Users

To view a list of locally-defined users, do the following:

- Choose **Management Appliance > System Administration > Users**.



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 custom user roles, see [Custom User Roles](#) , on page 406.

Setting and Changing Passphrases

- When you add a user, you specify an initial passphrase for that user.
- To change passphrases for users configured on the system, use the Edit User page in the GUI (see [Editing Locally-Defined Users](#), on page 415 for more information).



Note Cisco recommends you to change the passphrase when you log in to the appliance for the first time or after you complete the System Setup Wizard.


- To change the passphrase for the default admin user account for the system, see [Changing the Admin User's Passphrase](#), on page 413.

- To force users to change their passphrases, see [Requiring Users to Change Passphrase on Demand](#), on page 420.
- Users can change their own passphrases by clicking the Options menu at the top right side of the GUI and selecting the Change Passphrase option.

Setting Passphrase and Login Requirements

You can define user account and passphrase restrictions to enforce organizational passphrase policies. The user account and passphrase restrictions apply to local users defined on the Security Management 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.
- **Passphrase lifetime rules.** You can define how long a passphrase can exist before the user is required to change the passphrase after logging in.
- **Passphrase rules.** You can define what kinds of passphrases users can choose, such as which characters are optional or mandatory.

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Users**.
- Step 3** Scroll down to the **Local User Account and Passphrase Settings** section.
- Step 4** Click **Edit Settings**.
- Step 5** Configure 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 passphrase 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>Note You can also manually lock individual user accounts. See Locking User Accounts Manually, on page 420.</p>

Setting	Description
Passphrase Reset	<p>Choose whether or not users should be forced to change their passphrases after an administrator changes their passphrases.</p> <p>You can also choose whether or not users should be forced to change their passphrases after they expire. Enter the number of days a passphrase can last before users must change it. You can enter any number from one (1) to 366. Default is 90. To force users to change their passphrases at non-scheduled times, see Requiring Users to Change Passphrase on Demand, on page 420.</p> <p>When you force users to change their passphrases after they expire, you can display a notification about the upcoming passphrase expiration. Choose the number of days before expiration to notify users.</p> <p>Note When a user account uses SSH keys instead of a passphrase challenge, the Passphrase Reset rules still apply. When a user account with SSH keys expires, the user must enter their old passphrase or ask an administrator to manually change the passphrase to change the keys associated with the account.</p>
Passphrase Rules: Require at least <number> characters.	<p>Enter the minimum number of characters that passphrases may contain.</p> <p>Enter any number between one (1) and 128.</p> <p>The default is 8.</p> <p>Passphrases can have more characters than the number you specify here.</p>
Passphrase Rules: Require at least one number (0-9).	<p>Choose whether or not the passphrases must contain at least one number.</p>
Passphrase Rules: Require at least one special character.	<p>Choose whether or not the passphrases must contain at least one special character. Passphrases may contain the following special characters:</p> <p>~ ? ! @ # \$ % ^ & * - _ + =</p> <p>\ / [] () < > { } ` ' " ; : , .</p>

Setting	Description
Passphrase Rules: Ban usernames and their variations as passphrases.	Choose whether or not the passphrase are allowed to be the same as the associated user name or variations on the user name. When user name variations are banned, the following rules apply to passphrases: <ul style="list-style-type: none"> • The passphrase may not be the same as the user name, regardless of case. • The passphrase may not be the same as the user name in reverse, regardless of case. • The passphrase may not be the same as the user name or reversed user name with the following character substitutions: <ul style="list-style-type: none"> • "@" or "4" for "a" • "3" for "e" • " ", "!", or "1" for "i" • "0" for "o" • "\$" or "5" for "s" • "+" or "7" for "t"
Passphrase Rules: Ban reuse of the last <number> passphrases.	Choose whether or not users are allowed to choose a recently used passphrase when they are forced to change the passphrase. If they are not allowed to reuse recent passphrases, enter the number of recent passphrase that are banned from reuse. You can enter any number from one (1) to 15. Default is three (3).
Passphrases Rules: List of words to disallow in passphrases	You can create a list of words to disallow in passphrases. Make this file a text file with each forbidden word on a separate line. Save the file with the name forbidden_passphrase_words.txt and use SCP or FTP to upload the file to the appliance. If this restriction is selected but no word list is uploaded, this restriction is ignored.

Setting	Description
Passphrase Strength	<p>You can display a passphrase-strength indicator when an admin or user enters a new passphrase.</p> <p>This setting does not enforce creation of strong passphrases, it merely shows how easy it is to guess the entered passphrase.</p> <p>Select the roles for which you wish to display the indicator. Then, for each selected role, enter a number greater than zero. A larger number means that a passphrase that registers as strong is more difficult to achieve. This setting has no maximum value.</p> <p>Examples:</p> <ul style="list-style-type: none"> • If you enter 30 , then an 8 character passphrase with at least one upper- and lower-case letter, number, and special character will register as a strong passphrase. • If you enter 18 , then an 8 character passphrase with all lower case letters and no numbers or special characters will register as strong. <p>Passphrase strength is measured on a logarithmic scale. Evaluation is based on the U.S. National Institute of Standards and Technology rules of entropy as defined in NIST SP 800-63, Appendix A.</p> <p>Generally, stronger passphrases:</p> <ul style="list-style-type: none"> • Are longer • Include upper case, lower case, numeric, and special characters • Do not include words in any dictionary in any language. <p>To enforce passphrases with these characteristics, use the other settings on this page.</p>
Passphrase Rule	<p>A new passphrase rule is added in your Email and Web Manager to define your login passphrase:</p> <p>Avoid usage of passphrases that contain three or more repetitive or sequential characters, (for example, 'AAA@124,' 'Abc@123,' and so on.)</p>
Passphrase Rule	<p>A new passphrase rule is added to your Email and Web Manager to define your login passphrase:</p> <p>Avoid usage of username substrings in your passphrase. Three or more characters from username along with numeric and special characters are not allowed.</p>

Step 6 Submit and commit your changes.


What to do next

Require users to change their passphrases to new passphrases that meet the new requirements. See [Requiring Users to Change Passphrase on Demand](#) , on page 420

Requiring Users to Change Passphrase on Demand

To require all or selected users to change their passphrases at any time on an ad-hoc basis, perform the steps in this procedure. This is a one-time action.

To automate a periodic requirement for changing passphrases, use the Passphrase Reset option described in [Setting Passphrase and Login Requirements](#) , on page 416.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Users**.
- Step 3** In the Users section, select the check boxes beside the users who will be required to change passphrases .
- Step 4** Select **Enforce Passphrase Changes**.
- Step 5** Select options.
The global setting for the grace period is configured in Local User Account & Passphrase Settings.
- Step 6** Click **OK**.
-


Locking and Unlocking Local User Accounts

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

- You can configure all local user accounts to lock after users fail to log in successfully after a configured number of attempts. See [Setting Passphrase and Login Requirements](#) , on page 416.
- Administrators can manually lock user accounts. See [Locking User Accounts Manually](#), on page 420.

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

Locking User Accounts Manually

- Step 1** First time only: Set up the appliance to enable user account locking:
- Step 2** Perform the following:
- a) [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - b) Go to **Management Appliance > System Administration > Users**.
 - c) In the **Local User Account & Passphrase Settings** section, click **Edit Settings**.
 - d) Select the checkbox to **Display Locked Account Message if Administrator has manually locked a user account** and enter your message.
 - e) Submit the change.
- Step 3** Go to **Management Appliance > System Administration > Users** and click the user name.
- Note** Before you lock the Admin account, be sure that you can unlock it. See the Note in [Unlocking User Accounts](#) , on page 421.
- Step 4** Click **Lock Account**.

AsyncOS displays a message saying that the user will be unable to log into the appliance and asks if you want to continue.

Unlocking User Accounts

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



Note If you lock the admin account, you can only unlock it by logging in as the admin through a serial communications connection to the serial console port. The admin user can always access the appliance using the serial console port, even when the admin account is locked. See the “Setup and Installation” chapter in the documentation or online help for your Email Security appliance for more information on accessing the appliance using the serial console port.

External User Authentication

If you store user information in an LDAP or RADIUS directory on your network, you can configure your Security Management appliance to use the external directory to authenticate users who log in to the appliance.



Note Some features described in [Customizing Your View](#), on page 542 are not available to externally-authenticated users.

- If your deployment uses both local and external authentication, local user names must not duplicate externally-authenticated user names.
- If the appliance cannot communicate with the external directory, a user who has both an external and a local account can log in with a local user account on the appliance.

See:

- [Configuring External Authentication of Administrative Users Using LDAP](#), on page 384
- [Enabling RADIUS Authentication](#), on page 421

Configuring LDAP Authentication

To configure LDAP authentication, see [Configuring External Authentication of Administrative Users Using LDAP](#), on page 384.

Enabling RADIUS Authentication


You can use a RADIUS directory to authenticate users and assign groups of users to user roles for administering your appliance. The RADIUS server should support the CLASS attribute, which AsyncOS uses to assign users in the RADIUS directory to user roles.



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.

Before you begin

The Shared Secret key for access to the RADIUS server must be no more than 48 characters long.

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance** > **System Administration** > **Users** page and click **Enable**.
- Step 3** Select the **Enable External Authentication** check box.
- Step 4** Select RADIUS for the authentication type.
- Step 5** Enter the host name for the RADIUS server.
- Step 6** Enter the port number for the RADIUS server. The default port number is 1812.
- Step 7** Enter the Shared Secret key for the RADIUS server.
- Note** When enabling external authentication for a cluster of Email Security appliances, enter the same Shared Secret key on all appliances in the cluster.
- Step 8** Enter the number of seconds that the appliance waits for a response from the server before timing out.
- Step 9** Select whether to use Passphrase Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) for the authentication protocol.
- Step 10** (Optional) Click **Add Row** to add another RADIUS server. Repeat Steps 6 and 7 for each RADIUS server that your appliance uses for authentication.
- When you define multiple external servers, the appliance connects to the servers in the order defined on the appliance. You might want to define multiple external servers to allow for failover in case one server is temporarily unavailable.
- Step 11** Enter the amount of time to store external authentication credentials in the web user interface.
- Note** If the RADIUS server uses one-time passphrases, for example passphrases created from a token, enter zero (0). When the value is set to zero, AsyncOS does not contact the RADIUS server again to authenticate during the current session.
- Step 12** Configure Group Mapping:

Setting	Description
Map externally authenticated users to multiple local roles (Recommended)	<p>AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements:</p> <ul style="list-style-type: none"> • 3 character minimum • 253 character maximum • no colons, commas, or newline characters • one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.) <p>For RADIUS users with multiple CLASS attributes, AsyncOS assigns the most restrictive role. For example, if a RADIUS user has two CLASS attributes, which are mapped to the Operator and Read-Only Operator roles, AsyncOS assigns the RADIUS user to the Read-Only Operator role, which is more restrictive than the Operator role.</p> <p>These are the appliance roles ordered from least restrictive to most restrictive:</p> <ul style="list-style-type: none"> • Administrator • Email Administrator • Web Administrator • Web Policy Administrator • URL Filtering Administrator (for web security) • Custom user role (email or web) <p>If a user is assigned multiple Class attributes that are mapped to custom user roles, the last class attribute on the list on the RADIUS server will be used.</p> <ul style="list-style-type: none"> • Technician • Operator • Read-Only Operator • Help Desk User • Guest
Map all externally authenticated users to the Administrator role	AsyncOS assigns RADIUS users to the Administrator role.

Step 13

(Optional) Click **Add Row** to add another group. Repeat step 11 for each group of users that the appliance authenticates.

Step 14

Submit and commit your changes.

Two-Factor Authentication

You can use a RADIUS directory to configure two-factor authentication for specific user roles. The appliance supports the following authentication protocols for communicating with the RADIUS server:

- Passphrase Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

You can enable two-factor authentication for the following user roles:

- predefined
- custom

The feature has been tested with:


- RSA Authentication Manager v8.2
- FreeRADIUS v1.1.7 and above
- ISE v1.4 and above

Related Topics:

- [Enabling Two-Factor Authentication, on page 424](#)
- [Disabling Two-Factor Authentication, on page 425](#)
- [Adding an Email or Web Security appliance over SSH with Pre-Shared Keys, on page 425](#)

Enabling Two-Factor Authentication

Make sure that you get the required RADIUS server details for two-factor authentication from your IT administrator.


-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **System Administration** > **Users** page and click **Enable** under Two-Factor Authentication.
- Step 3** Enter the hostname or IP address of the RADIUS server.
- Step 4** Enter the port number of the RADIUS server.
- Step 5** Enter the Shared Secret passphrase of the RADIUS server.
- Step 6** Enter the number of seconds to wait for a response from the server before timing out.
- Step 7** Select the appropriate authentication protocol.
- Step 8** (Optional) Click **Add Row** to add another RADIUS server. Repeat steps 2 to 6 for each RADIUS server.
- Note** You can add up to ten RADIUS servers.
- Step 9** Select the required user roles for which you want to enable two-factor authentication.
- Step 10** Submit and commit your changes.

When two-factor authentication is enabled, the user is prompted to enter a passcode after entering the username and passphrase, to login to the appliance.

Disabling Two-Factor Authentication

Before you begin

Make sure you have enabled two-factor authentication on your appliance.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 2** Choose **System Administration > Users** page and click **Edit Global Settings** under Two-Factor Authentication
 - Step 3** Deselect **Enable Two-Factor Authentication**.
 - Step 4** Submit and commit your changes.
-

Adding an Email or Web Security appliance over SSH with Pre-Shared Keys

The following example demonstrates how to add an Email Security appliance (testesa.example.com) to the Security Management appliance (testesma.example.com) over SSH using pre-shared keys.

To add a Web Security appliance, choose **WSA** when prompted to enter the type of Cisco appliance.

```
testesma.example.com> applianceconfig
```

```
Choose the operation you want to perform.
```

```
ADD - Add SMA Connection Parameters and Keys.  
EDIT - Edit an appliance.  
DELETE - Remove an appliance.  
TEST - Test that an appliance is properly configured.  
SERVICES - Configure the centralized services for an appliance.  
STATUS - Display the status of centralized services.  
PORT - Configure which port is used to communicate with remote appliances.
```

```
[> add
```

```
Please enter the type of Cisco appliance that this device is
```

- 1. ESA
- 2. WSA

```
[1]> 1
```

```
Enter the IP address or hostname of an appliance to transfer data with.  
(A hostname may be entered in this field, however it will be immediately  
resolved to an IP address when the form is submitted.)
```

```
[> IP address entered
```

```
Enter a name to identify this appliance
```

```
[> name of appliance
```

```
File transfer access via SSH is required to transfer reporting data, message logs,  
and quarantine safelist/blocklist data from appliances
```

```

Would you like to configure file transfer access for this appliance? [Y]>

Would you like to use a custom ssh port to connect to this appliance? [N]>

Would you like to connect an Email Security appliance using pre-shared keys?
Use this option if you have enabled two-factor authentication on the Email
Security appliance. [N]> yes

To add an Email Security appliance to the Content Security Management appliance
using pre-shared keys, log in to the Email Security appliance,
run the smaconfig > add command, enter the following details.

Host: vm10sma0006.qa

User Key:
AAAAB3NzaC1yc2EAAAADAQABAAQDg3kG9RHc4gVZxRe0orh5DW5Yje5UB9BpJqcTRQJoxUIAv2Xig
8q5geyaWHZcFoUxH61YQbPX3R8CVMYgJ8/QB/iunjkr3jowV/SCuBBikEFgj1zuxlsFhL0L487epEgbylgH0rfJ
gwSa2/6dhfyUayst6pT87CZGOQltgx7s51wc+ve770X3SglQD5bdYC4x9+gCX0wdwfhTH1+4/82jwYjK1lAEXc
O4k4TuZJEJnyBQ3YyCyVwXuDkXpI6xJDemxcc36e7Wwtpn3mn2VLaTG2/I38XwSvLYB6TcqmWnO1oGL+aD
wkKAKcuhYpz4NFr9myej1mhMk7ZAFxmRNxvT

```



Note Before you proceed to the next step, ensure that you have added the **Host** and **User Key** details to the Email or Web Security appliance. Commit the changes in your Email or Web Security appliance before continuing the process of adding connection parameters in the Security Management appliance.

```

Do you want to continue connecting using pre-shared keys? [Y]> yes

```

Additional Controls on Access to the Security Management Appliance

- [Configuring IP-Based Network Access, on page 426](#)
- [Configuring the Web UI Session Timeout, on page 429](#)

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, on page 426](#)
- [Connecting Through a Proxy, on page 427](#)
- [Creating the Access List, on page 427](#)

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. The following figure shows the Network Access page with a list of user IP addresses that are allowed to connect directly to the Security Management appliance.

The following settings are applicable for the legacy web interface and the new web interface of the appliance.

Figure 12: Example Network Access Settings

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.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **System Administration > Network Access**.
- Step 3** Click **Edit Settings**.
- Step 4** Select the mode of control for the access list.
- Step 5** 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 6** 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 7** 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 spam quarantine sessions, which have a 30 minute timeout that cannot be configured.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Use the **System Administration > Network Access** page.
- Step 3** Click **Edit Settings**.
- Step 4** In the **Web UI Inactivity Timeout** field, 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 5 Submit and commit your changes.


Configuring the CLI Session Timeout

You can specify how long a user can be logged into the Security Management appliance's CLI before AsyncOS logs the user out due to inactivity. The CLI session timeout applies:

- To all users, including administrator
- Only to the connections using Secure Shell (SSH), SCP, and direct serial connection




Note Any uncommitted configuration changes at the time of CLI session timeout will be lost. Make sure that you commit the configuration changes as soon as they are made.

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Use the **System Administration > Network Access** page.
- Step 3** Click **Edit Settings**.
- Step 4** In the **CLI Inactivity Timeout** field, 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 5** Submit and commit your changes.
-

What to do next

You can also use the `adminaccessconfig` command in CLI to configure CLI session timeout. See *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.

Controlling Access to Sensitive Information in Message Tracking

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Go to the **Management Appliance > System Administration > Users** page.
- Step 3** In the **Tracking Privileges** section, click **Edit Settings**.
- Step 4** Select the roles for which you want to grant access to sensitive information in Message Tracking.
Only custom roles with access to Message Tracking are listed.
- Step 5** 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.

Displaying a Message for Administrative Users

You can display a message that administrative users will see when they sign in to the appliance.

To set or clear a message:

-
- Step 1** If you are planning to use a text file, upload it to the `/data/pub/configuration` directory on the appliance.
 - Step 2** Access the command-line interface (CLI).
 - Step 3** Run the `adminaccessconfig > BANNER` command.
 - Step 4** Load the banner message.
 - Step 5** Commit the change.

Enabling and Disabling Message Banners for Administrative Users

You can enable and disable a banner with a link to navigate to the new web interface of the appliance from the legacy web interface of the appliance.

-
- Step 1** Access the command-line interface (CLI).
 - Step 2** Run the `adminaccessconfig > NGUIBANNER` command.
 - Step 3** Enable or disable the banner message.
 - Step 4** Commit the change.

Viewing Administrative User Activity

- [Viewing Active Sessions Using the Web](#) , on page 431
- [Viewing Your Recent Login Attempts](#) , on page 432
- [Viewing Administrative User Activity via the Command Line Interface](#) , on page 432

Viewing Active Sessions Using the Web

From the Security Management appliance, you can view all active sessions and users logged in to the appliance.

From the upper right corner of the window, choose **Options > Active Sessions**.

Figure 13: Active Sessions Menu

Logged in as: **admin** on **m1**
Options ▾ Help a

Active Sessions

Active Sessions for m1060s02.sma

Username	Role	Login Time ▾	Idle Time	Remote Host	Interface
admin	Administrator	06 Aug 2010 21:10 (GMT +03:00)	25 secs	173.37.7.243	GUI

< Return to previous 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.

Viewing Your Recent Login Attempts

To view your last few recent login attempts (failed or successful) via the web interface, SSH, and/or FTP:

- Step 1** Log in.
- Step 2** Click the Figure-icon icon beside "Logged in as" near the top right side of the screen.

Viewing Administrative User Activity via the Command Line Interface

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 or the web user interface, the role of the user, the time of login, the idle time, and the remote host from which the user is logged in.
- 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	

Troubleshooting Administrative User Access

- [Error: User Has No Access Privileges Assigned, on page 433](#)
- [User Has No Active Menus , on page 433](#)
- [Externally-Authenticated Users See Preferences Option , on page 433](#)

Error: User Has No Access Privileges Assigned

Problem

A user to whom you have delegated administration can log in to the Security Management appliance but sees a message that no access privileges are assigned.

Solution

Make sure that you have assigned privileges to the custom user role to which this user is assigned. Look at Management Appliance > System Administration > Users to determine the User Role assigned, then go to Management Appliance > System Administration > User Roles, click the name of the User Role, and assign privileges to the role.

If you have assigned access based on Reporting Group, make sure you have selected a Reporting Group for that user on the Management Appliance > System Administration > User Roles page. To assign a group, click the **No groups selected** link in the Email Reporting column of the User Roles for Delegated Administration table.

User Has No Active Menus

Problem

A user to whom you have granted Publish privileges has no active menus upon login.

Solution

Make sure you have granted access to at least one Access Policy or Custom URL Category. If you do not want to grant this user privileges to edit either of these, create a custom URL category which is not used in any policy and grant this user role privileges to this category on the Custom User Role page.

Externally-Authenticated Users See Preferences Option

Problem

Externally-authenticated users see the Preferences option.

Solution

Ensure that users that you add directly in the Security Management appliance have unique usernames that are not also used in your external authentication database.



CHAPTER 17

Common Administrative Tasks

This chapter contains the following sections:

- [Performing Administrative Tasks](#), on page 436
- [Cisco Content Security Management Appliances Licensing](#), on page 436
- [Performing Maintenance Tasks Using CLI Commands](#), on page 468
- [Enabling Remote Power Cycling](#), on page 472
- [Monitoring System Health Using SNMP](#), on page 474
- [Backing Up Security Management Appliance Data](#), on page 476
- [Disaster Recovery on the Security Management Appliance](#), on page 482
- [Upgrading Appliance Hardware](#), on page 484
- [Upgrading AsyncOS](#), on page 484
- [About Reverting to an Earlier Version of AsyncOS](#), on page 495
- [About Updates](#), on page 497
- [Configuring the Appliance to Trust Proxy Server Communication](#), on page 497
- [Configuring the Return Address for Generated Messages](#), on page 499
- [Managing Alerts](#), on page 499
- [Changing Network Settings](#), on page 506
- [Secure Communication Protocol](#), on page 510
- [Configuring the System Time](#), on page 510
- [Configuration File Page](#), on page 513
- [Saving and Importing Configuration Settings](#), on page 513
- [Managing Disk Space](#), on page 521
- [Managing Data Storage Time](#), on page 524
- [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances](#), on page 525
- [SSO Using SAML 2.0](#), on page 525
- [Configuring OpenID Connect 1.0 on Cisco Content Security Management for AsyncOS APIs](#), on page 539
- [Customizing Your View](#), on page 542
- [Restarting and Viewing Status of Services Enabled on Appliance](#), on page 544
- [Managing Lists of Certificate Authorities](#), on page 546
- [Configuring CRL Sources](#), on page 548
- [Receiving and Delivering Messages with Internationalised Domain Names \(IDNs\)](#), on page 552
- [FQDN](#), on page 554
- [X.509 Certificate](#), on page 556

- [Single Pane of Glass](#) , on page 558

Performing 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 [Monitoring System Status](#), on page 363



Note Several of the features or commands described in this chapter can affect routing precedence. For more information, see [IP Addresses, Interfaces, and Routing](#), on page 618.

Cisco Content Security Management Appliances Licensing

- [Working with Feature Keys](#), on page 436
- [Smart Software Licensing](#), on page 437



Note From AsyncOS 15.5 release onwards, there will be **no support** for classic licensing for **On-Premises users**. You will no longer be able to order new feature licenses or renew existing feature licenses in the Classic Licensing mode.


Prerequisite: Make sure you create a smart account in the Cisco Smart Software Manager portal and enable Cisco Smart Software Licensing on your Secure Email and Web Manager. For more information, see [Smart Software Licensing](#), on page 437 .

From AsyncOS 15.5 release onwards, you can load the license using the `loadlicense` command only if the license file contains a cloud feature key.

If the license file does not contain a cloud feature key, you cannot load the license, and you will receive a notification message notifying you to retry with a cloud license or use `license_smart` command to perform Smart Licensing tasks.

Working with Feature Keys

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.

To	Do This
View all active feature keys for Secure Email and Web Manager	[New Web Interface Only] On the Cloud Email Security Management Console, click the gear  icon to load the legacy web interface. Select Management Appliance > System Administration > Feature Keys .

Smart Software Licensing

- [Overview, on page 437](#)
- [Enabling Smart Software Licensing, on page 441](#)
- [Registering the Appliance with Cisco Smart Software Manager, on page 441](#)
- [Obtaining and Using VLN, Certificate, and Key Details to Register Secure Email and Web Manager in Air-Gap Mode, on page 442](#)
- [Requesting for Licenses, on page 443](#)
- [Releasing Licenses, on page 443](#)
- [Deregistering the Appliance from Smart Cisco Software Manager , on page 444](#)
- [Reregistering the Appliance with Smart Cisco Software Manager , on page 444](#)
- [Changing Transport Settings, on page 444](#)
- [Renewing Authorization and Certificate, on page 444](#)
- [Reserving Feature Licenses, on page 445](#)
- [Updating Smart Agent, on page 449](#)
- [Alerts, on page 449](#)
- [Command Line Interface, on page 450](#)

Overview

Smart Software Licensing enables you to manage and monitor Cisco Content Security Management appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM) which is the centralized database that maintains the licensing details about all the Cisco products that you purchase and use. With Smart Licensing, you can register with a single token rather than registering them individually on the website using Product Authorization Keys (PAKs).

Once you register the appliance, you can track your appliance licenses and monitor license usage through the CSSM portal. The Smart Agent installed on the appliance connects the appliance with CSSM and passes the license usage information to the CSSM to track the consumption.

See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Cisco Smart Software Manager.

- Make sure that your appliance has internet connectivity.

- Contact Cisco sales team to create a smart account in Cisco Smart Software Manager portal (<https://software.cisco.com/#module/SmartLicensing>) or install a Cisco Smart Software Manager Satellite on your network.

See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know more about Cisco Smart Software Manager user account creation or installing a Cisco Smart Software Manager Satellite.

For users who do not want to directly send the license usage information to the internet, the Smart Software Manager Satellite can be installed on the premises, and it provides a subset of CSSM functionality. Once you download and deploy the satellite application, you can manage licenses locally and securely without sending data to CSSM using the internet. The CSSM Satellite periodically transmits the information to the cloud.



Note If you want to use Smart Software Manager Satellite, use Smart Software Manager Satellite Enhanced Edition 6.1.0.

- The existing users of classical licenses (traditional) should migrate their classical licenses to smart licenses. See <https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic>.
- The system clock of the appliance must be in sync with that of the CSSM. Any deviation in the system clock of the appliance with that of the CSSM, will result in failure of smart licensing operations.



Note If you have internet connectivity and want to connect to the CSSM through a proxy, you must use the same proxy that is configured for the appliance using **System Administration-> Update Settings**

License Reservation

You can reserve licenses for features enabled in Secure Email and Web Manager without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for users that deploy Secure Email and Web Manager in a highly secured network environment with no communication to the Internet or external devices.

The feature licenses can be reserved in any one of the following modes:

- **Specific License Reservation (SLR)** – use this mode to reserve licenses for individual features (for example, ‘Mail Handling’) for a given time-period.
- **Permanent License Reservation (PLR)** – use this mode to reserve licenses for all features permanently.

For more information on how to reserve the licenses in Secure Email and Web Manager, see [Reserving Feature Licenses, on page 445](#).

Device Led Conversion

After you register Secure Email and Web Manager with smart licensing, all existing, valid classical licenses are automatically converted to smart licenses using the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal.



Note The DLC process is initiated if Secure Email and Web Manager contains valid feature licenses.



Note After the DLC process is complete, you will not be able to convert the smart licenses to classical licenses. Contact Cisco TAC for assistance.



Note The DLC process takes approximately an hour to complete.

You can view the status of the DLC process – ‘success’ or ‘failed’ in any one of the following ways:

- Device Led Conversion status field under the 'Smart Software Licensing Status' section in the **System Administration > Smart Software Licensing** page of the web interface.
- Conversion Status entry in the `license_smart > status` sub command in the CLI.



Note When the DLC process fails, the system sends a system alert that details the reason for the failure. You need to fix the issue and then use the `license_smart > conversion_start` sub command in the CLI to manually convert the classical licenses to smart licenses.



Note The DLC process is applicable only for classical licenses and not for the SLR or PLR modes of license reservation.

Smart Software Licensing – New User

If you are a new (first-time) Smart Software Licensing user, you must perform the following procedures to activate Smart Software Licensing:

	Do This	More Informaton
Step 1	Enable Smart Software Licensing	Enabling Smart Software Licensing, on page 441
Step 2	Register the Secure Email and Web Manager with Cisco Smart Software Manager	Registering the Appliance with Cisco Smart Software Manager, on page 441
Step 3	Request for licenses (feature keys)	Requesting for Licenses, on page 443

Migrating from Classical Licensing to Smart Software Licensing - Existing User

If you are migrating from Classical Licensing to Smart Software Licensing, you must perform the following procedures to activate Smart Software Licensing:

	Do This	More Informaton
Step 1	Enable Smart Software Licensing	Enabling Smart Software Licensing, on page 441
Step 2	Register the Secure Email and Web Manager with Cisco Smart Software Manager	Registering the Appliance with Cisco Smart Software Manager, on page 441
Step 3	Request for licenses (feature keys)	Requesting for Licenses, on page 443

Note: After you register Secure Email and Web Manager with Smart Software Licensing, all existing, valid Classical Licenses are automatically converted to Smart Licenses using the Device Led Conversion (DLC) process. For more information, see [Device Led Conversion](#), on page 438.

Smart Software Licensing in Air-Gap Mode – New User

If you are using Secure Email and Web Manager operating in air-gap mode, and if you are activating Smart Software Licensing for the first-time, you must perform the following procedures:

	Do This	More Informaton
Step 1	Enable Smart Software Licensing	Enabling Smart Software Licensing, on page 441
Step 2	Obtaining and Using VLN, Certificate, and Key Details to Register Secure Email and Web Manager in Air-Gap Mode for the first-time	Obtaining and Using VLN, Certificate, and Key Details to Register Secure Email and Web Manager in Air-Gap Mode, on page 442
Step 3	Request for licenses (feature keys)	Requesting for Licenses, on page 443

Smart Software Licensing in Air-Gap Mode – Existing User

If you are using Secure Email and Web Manager operating in air-gap mode, you must perform the following procedures to activate Smart Software Licensing:

	Do This	More Informaton
Step 1	Enable Smart Software Licensing	Enabling Smart Software Licensing, on page 441
Step 2	Register Secure Email and Web Manager operating in air-gap mode with license reservation	Reserving Feature Licenses, on page 445

	Do This	More Informaton
Step 3	Request for licenses (feature keys)	Requesting for Licenses, on page 443

Enabling Smart Software Licensing

Step 1 Choose **Managed Appliance > System Administration > Smart Software Licensing**.

Step 2 Click **Enable Smart Software Licensing**.

To know about Smart Software Licensing, click on the Learn More about Smart Software Licensing link.

Step 3 Click **OK** after reading the information about Smart Software Licensing.

Step 4 Commit your changes.

What to do next

After you enable Smart Software Licensing, all the features in the Classic Licensing mode will be automatically available in the Smart Licensing mode. If you are an existing user in Classic Licensing mode, you have 90-days evaluation period to use the Smart Software Licensing feature without registering your appliance with the CSSM.

You will get notifications on regular intervals (90th, 60th, 30th, 15th, 5th, and last day) prior to the expiry and also upon expiry of the evaluation period. You can register your appliance with the CSSM during or after the evaluation period.



Note New Virtual Appliance users with no active licenses in Classic Licensing mode will not have the evaluation period even if they enable the Smart Software Licensing feature. Only the existing Virtual Appliance users with active licenses in Classic Licensing mode will have evaluation period. If new Virtual Appliance users want to evaluate the smart licensing feature, contact Cisco Sales team to add the evaluation license to the smart account. The evaluation licenses are used for evaluation purpose after registration.



Note After you enable the Smart Licensing feature on your appliance, you will not be able to roll back from Smart Licensing to Classic Licensing mode.

Registering the Appliance with Cisco Smart Software Manager

You must enable the Smart Software Licensing feature under System Administration menu in order to register your appliance with the Cisco Smart Software Manager.

Step 1 Go to **Managed Appliance > System Administration > Smart Software Licensing**.

Step 2 Select the **Smart License Registration** option.

Step 3 Click **Confirm**.

- Step 4** Click **Edit**, if you want to change the **Transport Settings**. The available options are:
- **Direct**: Connects the appliance directly to the Cisco Smart Software Manager through HTTPs. This option is selected by default.
 - **Transport Gateway**: Connects the appliance to the Cisco Smart Software Manager through a Transport Gateway or Smart Software Manager Satellite. When you choose this option, you must enter the URL of the Transport Gateway or the Smart Software Manager Satellite and click OK. This option supports HTTP and HTTPS. In FIPS mode, Transport Gateway supports only HTTPS. See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Transport Gateway.
- Access the Cisco Smart Software Manager portal (<https://software.cisco.com/#module/SmartLicensing> using your login credentials. Navigate to the Virtual Account page of the portal and access the General tab to generate a new token. Copy the Product Instance Registration Token for your appliance.
- See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Product Instance Registration Token creation.
- Step 5** Switch back to your appliance and paste the Product Instance Registration Token.
- Step 6** Click **Register**.
- Step 7** On the Smart Software Licensing page, you can check the Reregister this product instance if it is already registered check box to reregister your appliance. See [Reregistering the Appliance with Smart Cisco Software Manager](#) , on page 444.

What to do next

The product registration process takes a few minutes and you can view the registration status on the Smart Software Licensing page.



Note After you enabled smart software licensing and registered your content security gateway with the Cisco Smart Software Manager, the Cisco Cloud Services portal is automatically enabled and registered on your content security gateway.

Obtaining and Using VLN, Certificate, and Key Details to Register Secure Email and Web Manager in Air-Gap Mode

Perform the following steps to obtain VLN, certificate, and key details and use these details to register your virtual Secure Email and Web Manager operating in air-gap mode:

- Step 1** Register a virtual Secure Email and Web Manager operating outside the air-gap mode. For information on how to register a virtual Secure Email and Web Manager, see [Registering the Appliance with Cisco Smart Software Manager](#), on page 441.
- Step 2** Enter the `vlinfo` command in the CLI. This command displays the VLN, certificate, and key details. Copy these details and maintain these details to use it later.
- Note** The `vlinfo` command is available in Smart Licensing mode. For more information on the `vlinfo` command, see [vlinfo](#), on page 466.

- Step 3** Register your virtual Secure Email and Web Manager operating in air-gap mode with your license reservation. For more information on how to register a virtual Secure Email and Web Manager with your license reservation, see [Reserving Feature Licenses, on page 445](#).
- Step 4** Enter `updateconfig > VLNID` subcommand in the CLI.
- Step 5** Paste the copied VLN (in step 2) when you are prompted to enter the VLN.
- Note** The `updateconfig > VLNID` subcommand is available only in License Reservation mode. For more information on how to use `updateconfig -> VLNID` subcommand, see [updateconfig, on page 464](#).
- Note** Using the `VLNID` subcommand, you can add or update the VLNID. The update option is available to modify the VLN if you enter an incorrect VLN.
- Step 6** Enter `CLIENTCERTIFICATE` command in the CLI.
- Step 7** Paste the copied certificate and key details (in step 2) when you are prompted to enter these details.

Requesting for Licenses

Once you complete the registration process successfully, you must request for licenses for the Secure Email and Web Manager's features as required.



Note In License Reservation mode (air-gap mode), you must request for licenses before the license token is applied to the Secure Email and Web Manager.

- Step 1** Choose **Management Appliance > System Administration > Licenses**.
- Step 2** Click **Edit Settings**.
- Step 3** Check the checkboxes under the License Request/Release column corresponding to the licenses you want to request for.
- Step 4** Click **Submit**.
- Note** By default the license for Mail Handling is available. You cannot activate, deactivate, or release this license. There is no evaluation period or out of compliance for Mail Handling license.

What to do next

When the licenses are overused or expired, they will go to out of compliance (OOC) mode and 30-days grace period is provided to each license. You will get notifications on regular intervals (30th, 15th, 5th, and last day) prior to the expiry and also upon the expiry of the OOC grace period.

After the expiry of the OOC grace period, you cannot use the licenses and the features will be unavailable. To access the features again, you must update the licenses on the CSSM portal and renew the authorization.

Releasing Licenses

- Step 1** Choose **Management Appliance > System Administration > Licenses**.

Step 2 Click **Edit Settings**.

Step 3 Uncheck the checkboxes under the License Request column corresponding to the licenses you want to release.

Step 4 Click **Submit**.

Note You cannot release the license for Mail Handling.

Deregistering the Appliance from Smart Cisco Software Manager

Step 1 Choose **Management Appliance > System Administration > Smart Software Licensing**.

Step 2 From the **Action** drop-down list, choose **Deregister** and click **Go**.

Step 3 Click **Submit**.

Reregistering the Appliance with Smart Cisco Software Manager

Step 1 Choose **Management Appliance > System Administration > Smart Software Licensing**.

Step 2 From the **Action** drop-down list, choose **Reregister** and click **Go**.

What to do next

See [Registering the Appliance with Cisco Smart Software Manager, on page 441](#) to know about registration process.

You can reregister the appliance after you reset the appliance configurations during unavoidable scenarios.

Changing Transport Settings

You can change the transport settings only before registering the appliance with CSSM.



Note You can change the transport settings only when the smart licensing feature is enabled. If you have already registered your appliance, you must deregister the appliance to change the transport settings. After changing the transport settings, you must register the appliance again.

See [Registering the Appliance with Cisco Smart Software Manager, on page 441](#) to know how to change the transport settings.

Renewing Authorization and Certificate

After you register your appliance with the Smart Cisco Software Manager, you can renew the certificate.



Note You can renew authorization only after the successful registration of the appliance.

Step 1 Choose **Management Appliance > System Administration > Smart Software Licensing**.

Step 2 From the **Action** drop-down list, choose the appropriate option:

- **Renew Authorization Now**
- **Renew Certificates Now**

Step 3 Click **Go**.

Reserving Feature Licenses

- [Enabling License Reservation, on page 445](#)
- [Registering License Reservation, on page 446](#)
- [Updating License Reservation, on page 447](#)
- [Removing License Reservation, on page 448](#)
- [Disabling License Reservation, on page 449](#)

Enabling License Reservation

Before you begin

Make sure you have already enabled the Smart Licensing mode in Secure Email and Web Manager.



Note You can also enable the license reservation using the `license_smart > enable_reservation` sub command in the CLI. For more information, see the ‘Smart Software Licensing’ section in ‘The Commands: Reference Examples’ chapter of the CLI Reference Guide.

Step 1 Go to **System Administration > Smart Software Licensing** page in Secure Email and Web Manager.

Step 2 Select the **Specific/Permanent License Reservation** option.

Step 3 Click **Confirm**.

The license reservation (SLR or PLR) is enabled in Secure Email and Web Manager.

What to do next

- You need to register the license reservation. For more information, see [Registering License Reservation, on page 446](#).

- You can disable the license reservation in Secure Email and Web Manager, if required. For more information, see [Disabling License Reservation, on page 449](#).

Registering License Reservation

Before you begin

Make sure you have already enabled the required license reservation (SLR or PLR) in Secure Email and Web Manager.



Note You can also register the feature licenses using the `license_smart > request_code` and `license_smart > install_authorization_code` sub commands in the CLI.

Step 1 Go to **System Administration > Smart Software Licensing** page in Secure Email and Web Manager.

Step 2 Click **Register**.

Step 3 Click **Copy Code** to copy the request code.

Note You need to use the request code in the CSSM portal to generate an authorization code.

Note A system alert is sent every 24 hours to indicate that you need to install an authorization code.

Step 4 Click **Next**.

Note The request code is canceled when you click the Cancel button. You cannot install the authorization code (generated in the CSSM portal) in Secure Email and Web Manager. Contact Cisco TAC to assist you in removing the reserved license after the request code is canceled in Secure Email and Web Manager.

Step 5 Go to the CSSM portal to generate an authorization code to reserve licenses for specific or all features.

Note For more information on how to generate an authorization code, go to the *Inventory: License Tab > Reserve Licenses* section of the Help documentation at [Smart Software Licensing Online Help \(cisco.com\)](#).

Step 6 Paste the authorization code obtained from the CSSM portal in Secure Email and Web Manager in any one of the following ways:

- Select the **Copy and Paste authorization code** option and paste the authorization code in the text box under the 'Copy and Paste authorization code' option.
- Select the **Upload authorization code from the system** option and click **Choose File** to upload the authorization code.

Step 7 Click **Install Authorization Code**.

Note After you install the authorization code, you receive a system alert that indicates Smart Agent successfully installed the license reservation.

The license reservation (SLR or PLR) is registered in Secure Email and Web Manager. In SLR, only the reserved license is moved to the 'Reserved in Compliance' state. For PLR, all licenses in Secure Email and Web Manager are moved to the 'Reserved in Compliance' state.



Note The 'Reserved In Compliance:' state indicates that Secure Email and Web Manager is authorized to use the license.

What to do next

- [Applicable for SLR only]: You can update the license reservation, if required. For more information, see [Updating License Reservation, on page 447](#).
- [Applicable for SLR and PLR]: You can remove the license reservation, if required. For more information, see [Removing License Reservation, on page 448](#).
- You can disable the license reservation in Secure Email and Web Manager, if required. For more information, see [Disabling License Reservation, on page 449](#).

Updating License Reservation

You can reserve license for a new feature or modify the existing license reservation for a feature.



Note You can only update the Specific License reservations and not the Permanent License reservations.



Note You can also update the license reservation using the `license_smart > reauthorize` sub command in the CLI.

-
- Step 1** Go to the CSSM portal to generate an authorization code to update the already reserved licenses.
- Note** For more information on how to generate an authorization code, go to the *Inventory: Product Instances Tab > Update Reserved Licenses* section of the Help documentation at [Smart Software Licensing Online Help \(cisco.com\)](#).
- Step 2** Copy the authorization code obtained from the CSSM portal.
- Step 3** Go to **System Administration > Smart Software Licensing** page in Secure Email and Web Manager.
- Step 4** Select **Reauthorize** from the 'Action' drop-down list and click **GO**.
- Step 5** Paste the authorization code obtained from the CSSM portal in Secure Email and Web Manager in any one of the following ways:
- Select the **Copy and Paste authorization code** option and paste the authorization code in the text box under the 'Copy and Paste authorization code' option.
 - Select the **Upload authorization code from the system** option and click **Choose File** to upload the authorization code.
- Step 6** Click **Re-authorize**.
- Step 7** Click **Copy Code** to copy the confirmation code.
- Note** You need to use the confirmation code in the CSSM portal to update the license reservations.

Step 8 Click **OK**.

Step 9 Add the confirmation code obtained from Secure Email and Web Manager in the CSSM portal.

Note For more information on how to add the confirmation code, go to the *Inventory: Product Instances Tab > Update Reserved Licenses* section of the Help documentation at [Smart Software Licensing Online Help \(cisco.com\)](https://www.cisco.com/SmartSoftwareLicensingOnlineHelp).

The license reservations are updated. The reserved license is moved to the 'Reserved in Compliance' state. The licenses that are not reserved are moved to the "Not Authorized" state.



Note The 'Not Authorized' state indicates that Secure Email and Web Manager has not reserved any feature licenses.

What to do next

- [Applicable for SLR and PLR]: You can remove the license reservation, if required. For more information, see [Removing License Reservation, on page 448](#).
- You can disable the license reservation in Secure Email and Web Manager. For more information, see [Disabling License Reservation, on page 449](#).

Removing License Reservation

You can remove the specific or permanent license reservation for the features enabled in Secure Email and Web Manager.



Note You can also remove the license reservation using the `license_smart > return_reservation` sub command in the CLI.

Step 1 Go to **System Administration > Smart Software Licensing** page in Secure Email and Web Manager.

Step 2 Select **Return code** from the 'Action' drop-down list and click **GO**.

Step 3 Click **Copy Code** to copy the return code.

Note You need to use the return code in the CSSM portal to remove the license reservations.

Note An alert is sent to the user to indicate that Smart Agent successfully generated the return code for the product.

Step 4 Click **OK**.

Step 5 Add the return code obtained from Secure Email and Web Manager in the CSSM portal.

Note For more information on how to add the return code, go to the *Inventory: Product Instances Tab > Removing a Product Instance* section of the Help documentation at [Smart Software Licensing Online Help \(cisco.com\)](https://www.cisco.com/SmartSoftwareLicensingOnlineHelp).

The licenses reserved in Secure Email and Web Manager are removed and moved to the evaluation period.

Disabling License Reservation

You can disable the license reservation in Secure Email and Web Manager.



Note You can also disable the license reservation using the `license_smart > disable_reservation` sub command in the CLI.

Step 1 Go to **System Administration > Smart Software Licensing** page in Secure Email and Web Manager.

Step 2 Click **Change Type** under the 'Registration Mode' field.

Step 3 Click **Submit** in the 'Change registration mode' dialog box.

The license reservation is disabled on Secure Email and Web Manager.

Updating Smart Agent

To update the Smart Agent version installed on your appliance, perform the following steps:

Step 1 Choose **Management Appliance > System Administration > Smart Software Licensing**.

Step 2 In the **Smart Agent Update Status** section, click **Update Now** and follow the process.

Note If you try to save any configuration changes using the CLI command `saveconfig` or through the web interface using **System Administration > Configuration Summary**, then Smart Licensing related configuration will not be saved.

Alerts

You will receive notifications on the following scenarios:

- Smart Software Licensing successfully enabled
- Smart Software Licensing enabling failed
- Beginning of the evaluation period
- Expiry of evaluation period (on regular intervals during evaluation period and upon expiry)
- Successfully registered
- Registration failed
- Successfully authorized
- Authorization failed
- Successfully deregistered
- Deregistration failed

- Successfully renewed Id certificate
- Renewal of Id certificate failed
- Expiry of authorization
- Expiry of Id certificate
- Expiry of out of compliance grace period (on regular intervals during out of compliance grace period and upon expiry).
- First instance of the expiry of a feature
- [Applicable for SLR and PLR only]: Authorization code is installed after generation of request code.
- [Applicable for SLR and PLR only]: Authorization code is installed successfully.
- [Applicable for SLR and PLR only]: Return code is generated successfully.
- [Applicable for SLR only]: Reservation of specific feature license is expired.
- [Applicable for SLR only]: Frequency of alerts sent before expiry of specific feature license reserved.

Command Line Interface

- [license_smart](#), on page 450
- [showlicense_smart](#), on page 458
- [cloudserviceconfig](#), on page 458
- [updateconfig](#), on page 464
- [vlninfo](#), on page 466
- [help vlninfo](#), on page 467

license_smart

- [Description](#), on page 451
- [Usage](#), on page 451
- [Example: Configuring Port for Smart Agent Service](#), on page 451
- [Example: Enabling Smart Licensing](#), on page 451
- [Example: Registering the Appliance with the Smart Software Manager](#) , on page 452
- [Example: Status of Smart Licensing](#) , on page 452
- [Example: Status Summary of Smart Licensing](#) , on page 452
- [Example: Setting the Smart Transport URL](#), on page 453
- [Example: Requesting Licenses](#), on page 453
- [Example: Releasing Licenses](#), on page 453
- [Example - Enabling and Registering License Reservation](#), on page 454

- [Example - Updating License Reservation, on page 455](#)
- [Example - Removing License Reservation, on page 456](#)
- [Example - Disabling License Reservation, on page 457](#)
- [Example - Enabling Device Led Conversion Process Manually, on page 457](#)

Description

Configure smart software licensing feature.

Usage

Commit: This command requires a 'commit'.

Batch Command: This command supports a batch format. For details, see the inline help by typing the command: `help license_smart`.

Example: Configuring Port for Smart Agent Service

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[ ]> setagentport

Enter the port to run smart agent service.
[65501]>
```

Example: Enabling Smart Licensing

```
mail.example.com > license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
[ ]> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
   in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
[Y/N] [ ]> y

> commit

Please enter some comments describing your changes:
[ ]>
Do you want to save the current configuration for rollback? [Y]>
```

Example: Registering the Appliance with the Smart Software Manager*Example: Registering the Appliance with the Smart Software Manager*

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTElMzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
OXhuenN4OWZDdktFckJlQzF5V3VibzkyTFgx%0AQWcvaz0%3D%0A
Product registration is in progress. Use license_smart > status command to check status of
registration.
```

Example: Status of Smart Licensing

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Example: Status Summary of Smart Licensing

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[> summary

FeatureName LicenseAuthorizationStatus
```

Mail Handling
Content Security Management Master ISQ

In Compliance
In Compliance

Example: Setting the Smart Transport URL

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

```
[> url
```

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager satellite.

Choose from the following menu options:

```
[1]> 1
```

Note: The appliance uses the Direct URL

(<https://smartreceiver.cisco.com/licservice/license>) to communicate with Cisco Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command. Transport settings will be updated after commit.

Example: Requesting Licenses



Note Users of virtual appliance must register their appliance to request for or release the licenses.

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

```
[> requestsmart_license
```

Feature Name	License Authorization Status
1. Content Security Management Centralized Tracking	Not Requested
2. Content Security Management Master ISQ	Not requested

Enter the appropriate license number(s) for activation.

Separate multiple license with comma or enter range:

```
[> 1
```

Activation is in progress for following features:

Security Management Centralized Tracking

Use license_smart > summary command to check status of licenses.

Example: Releasing Licenses

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

Example - Enabling and Registering License Reservation

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

```
[> releasesmart_license
```

Feature Name	License Authorization Status
1. Content Security Management Centralized Tracking	In Compliance
2. Content Security Management Master ISQ	In Compliance

Example - Enabling and Registering License Reservation

In this example, you can use the `license_smart>enable_reservation` sub command to enable and register the license reservation on Secure Email and Web Manager.

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure Email and Web Manager.

```
[> enable_reservation
```

Would you like to reserve license, then type "Y" else type "N" [Y/N] [> **yes**

License Reservation is enabled for the following machines:
mail1.example.com

License Reservation is enabled

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.

```
[> request_code
```

The generation of the request code is initiated...

Copy the request code obtained on your Secure Email and Web Manager and paste it in the Cisco Smart Software Manager portal to select the required license

Request code: CD-ZSMA:BD20B624E904-B7HCL9scQ-DD

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent license reservations on your Secure Email and Web Manager.

```

- CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Email and Web
Manager.
[]> install_authorization_code
1. Paste via CLI
2. Import the Authorization Code from a file

How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<pid>7b654af6-9d60-46f5-a79-.....PS/o+6</signature><udi>P:SMA,S:BE30B124E904
</udi></specificPLR>
^D
The SPECIFIC license reservation is successfully installed on your Secure Email and Web
Manager
Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
Email and Web Manager.
[]>

```

Example - Updating License Reservation

In this example, you can use the `license_smart > reauthorize` sub command to reserve license for a new feature or modify the existing license reservation for a feature.

```
mail.example.com > license_smart
```

```

Choose the operation you want to perform:
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
Email and Web Manager.
- REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Email and Web Manager.
- CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web
Manager.
- RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
Email and Web Manager.
[]> reauthorize

```

```

1. Paste via CLI
2. Import the Authorization Code from a file
How would you like to install Authorization Code?
[1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<pid>6b684af8-4d20-42f5-ab89-.....</authorizationCode><signature>
MEYCIDS7IZQuLvMMmiXMH2eZOWf7cy6rjgc7kxBIja</signature><udi>P:SMA,S:BD660B174E904
</udi></specificPLR>
^D

The SPECIFIC license reservation is successfully installed on your Secure Email and Web
Manager.

```

Example - Removing License Reservation

Copy the confirmation code obtained from Smart Agent and add it to the Cisco Smart Software Manager portal to update the specific reservation.

Confirmation code: 1f87b235

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
 - SUMMARY - Show Smart Licensing status summary.
 - DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure Email and Web Manager.
 - REAUTHORIZE - Install the authorization code to update specific or permanent license reservations on your Secure Email and Web Manager.
 - CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web Manager.
 - RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure Email and Web Manager.
- []>

Example - Removing License Reservation

In this example, you can use the `license_smart > return_reservation` sub command to remove the specific or permanent license reservation for the features enabled in Secure Email and Web Manager.

mail.example.com > **license_smart**

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
 - SUMMARY - Show Smart Licensing status summary.
 - DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure Email and Web Manager.
 - REAUTHORIZE - Install the authorization code to update specific or permanent license reservations on your Secure Email and Web Manager.
 - CONFIRM_CODE - Provide the confirmation code generated on your Secure Email and Web Manager.
 - RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure Email and Web Manager.
- []> **return_reservation**

After you return the license reservation, you cannot use any of the product features, if the evaluation period has exceeded 90 days. After the 90 days evaluation period, you must register your product with Cisco Smart Software Manager to continue to use the product features. [N]> **yes**

The generation of the return code is initiated...

Copy the return code obtained on your Secure Email and Web Manager and paste it in the Cisco Smart Software Manager portal.

Return Code: C97xKY-otSY8D-ertAf-v-fbEu5q-APo

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
 - SUMMARY - Show Smart Licensing status summary.
 - DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure Email and Web Manager.
 - REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- []>

mail1.example.com>

Example - Disabling License Reservation

In this example, you can use the `license_smart > disable_reservation` sub command to disable the license reservation on Secure Email and Web Manager .

```
mail.example.com > license_smart
```

Choose the operation you want to perform:

- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure Email and Web Manager.
- REQUEST_CODE - Provide the request code generated on your Secure Email and Web Manager.
- INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent license reservations on your Secure Email and Web Manager.
- CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Email and Web Manager.

```
[ ]> disable_reservation
```

A request code for the specific or permanent reservation is generated on your Secure Email and Web Manager. If you want to disable the reservation, it cancels the request code.

```
Do you want to disable the specific or permanent reservation? [Y/N] [ ]> yes
```

```
License Reservation is disabled for the following machines:  
mail1.example.com
```

```
License Reservation is disabled
```

Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure Email and Web Manager.

```
[ ]>
```

Example - Enabling Device Led Conversion Process Manually

In this example, you can use the `license_smart > conversion_start` sub command to enable the Device Led Conversion (DLC) process manually on Secure Email and Web Manager.

```
mail.example.com > license_smart
```

```
Deregister Secure Email and Web Manager from the Cisco Smart Software Manager portal to  
enable the license reservation
```

Choose the operation you want to perform:

- URL - Set the Smart Transport URL.
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- DEREGISTER - Deregister the product from Smart Licensing.
- REREGISTER - Reregister the product for Smart Licensing.
- RENEW_AUTH - Renew authorization of Smart Licenses in use.
- RENEW_ID - Renew registration with Smart Licensing.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- CONVERSION_START - To manually convert the classic license keys to smart Licensing

```
[ ]> conversion_start
```

showlicense_smart

```
Do you want to start the process of converting your classic license keys to smart software
licensing[Y/N]? []> yes
```

showlicense_smart

- [Description, on page 458](#)
- [Example: Status of Smart Licensing, on page 458](#)
- [Example: Status Summary of Smart Licensing, on page 458](#)

Description

Show Smart Licensing status and summary of status.

Example: Status of Smart Licensing

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Example: Status Summary of Smart Licensing

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> summary
```

FeatureName	LicenseAuthorizationStatus
Mail Handling	In Compliance
Content Security Management Master ISQ	In Compliance

cloudserviceconfig

- [Description, on page 459](#)
- [Usage, on page 459](#)
- [Example: Enabling Cisco Cloud Services on Appliance, on page 459](#)
- [Example: Disabling Cisco Cloud Services on Appliance, on page 460](#)

- [Example: Registering Content Security Gateway with Cisco Cloud Services Portal, on page 460](#)
- [Example: Deregistering Content Security Gateway from Cisco Cloud Services Portal, on page 461](#)
- [Example: Choosing Cisco Secure Cloud Server to connect Content Security Gateway to Cisco Cloud Services Portal, on page 461](#)
- [Example: Enabling Cisco SecureX or Cisco Threat Response on Content Security Gateway , on page 464](#)
- [Example: Disabling Cisco SecureX or Cisco Threat Response on Content Security Gateway , on page 464](#)

Description

The **cloudserviceconfig** command is used to:

- This command is applicable only in Smart Licensing mode.
- Enable the Cisco Cloud Services portal on your appliance.
- Disable the Cisco Cloud Services portal on your appliance.
- Register your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.
- Automatically register your Cisco Secure Email and Web Manager with the Cisco Cloud Services portal.
- Deregister your Cisco Secure Email and Web Manager from the Cisco Cloud Services portal.
- Choose the Cisco Secure Cloud server to connect your appliance to the Cisco Cloud Services portal.
- Fetch the certificate and key from talos server used by the updater.
- Enable Cisco SecureX (or Cisco Threat Response) on your Cisco Secure Email and Web Manager. You must perform this using the General configuration settings.
- Disable Cisco SecureX or Cisco Threat Response on your Cisco Secure Email and Web Manager. You must perform this using the General configuration settings.

Usage

- **Commit:** This command does not require a 'commit'.
- **Batch Command:** This command supports a batch format.

Example: Enabling Cisco Cloud Services on Appliance

In the following example, you can use the `cloudserviceconfig > enable` sub command to enable Cisco Cloud Services on your email gateway.



Note You can only use this sub command if Smart Software licensing is not enabled, and your appliance is not registered with Cisco Smart Software Manager

```
mail1.example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
```

Example: Disabling Cisco Cloud Services on Appliance

```

[ ]> enable
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[ ]> 1
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
maill.example.com > commit
Please enter some comments describing your changes:
[ ]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMT
maill.example.com >

```

Example: Disabling Cisco Cloud Services on Appliance

In the following example, you can use the `cloudserviceconfig > disable` sub command to disable Cisco Cloud Services on your appliance.

```

maill.example.com> cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[ ]> disable
The Cisco Cloud Service is currently disabled on your appliance.
maill.example.com > commit
Please enter some comments describing your changes:
[ ]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
maill.example.com >

```

Example: Registering Content Security Gateway with Cisco Cloud Services Portal

```

sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is stage-api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[ ]> REGISTER

Enter a registration token key to register your appliance with the Cisco Cloud Service
portal.
[ ]> 90a92909fc3b1be666f180621146fea3

The appliance registration is in progress.

```

Example: Deregistering Content Security Gateway from Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > deregister` sub command to deregister your appliance from the Cisco Cloud Services portal.

```
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
The Content Security Management appliance is successfully registered with the Cisco Cloud
Service portal.
Currently used Cisco Cloud Server is stage-api-sse.cisco.com

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
- ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
[ ]> DEREGISTER

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> Y

The Content Security Management appliance deregistration is in progress.
```

Example: Choosing Cisco Secure Cloud Server to connect Content Security Gateway to Cisco Cloud Services Portal

In the following example, you can use the `cloudserviceconfig > settrs` sub command to choose the required Cisco Secure Cloud Server to connect your email gateway to the Cisco Cloud Services portal.

```
mail1.example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[ ]> settrs
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[ ]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
mail1.example.com > commit
Please enter some comments describing your changes:
[ ]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT
```

Example Performing AutoRegistration using CLI for Smart Licensing

In the following example, you can use the command to display after you register once in smart licensing, the appliance performs auto registration in backend. If auto registration fails, you can see command for autoregistration in the CLI.

```
Autoregister Success/ and failure
sma> cloudserviceconfig

Cisco Cloud Service portal list update was successful.
```

Example Download a Certificate and Key

The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- REGISTER - To register the appliance with the Cisco Cloud Service portal.
 - SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
 - UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
 - AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically.
 - ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
- [> AUTOREGISTER

The appliance failed to auto-register with the Cisco Cloud Service portal.
Reason: A request to generate a Smart Licensing payload from Cisco Smart Software Manager failed.

The appliance is not registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- REGISTER - To register the appliance with the Cisco Cloud Service portal.
 - SETTRS - Set the Cisco Cloud Service portal to connect to the Cisco Cloud Service portal.
 - UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
 - AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically.
 - ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
- [> AUTOREGISTER

The appliance successfully auto-registered with the Cisco Cloud Service portal.

Example Download a Certificate and Key

In the following example, you can use the command to Fetch the certificate and key used by the updater from the TALOS server.

```
sma> cloudserviceconfig
```

Cisco Cloud Service portal list update was successful.
The Content Security Management appliance is successfully registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Choose the operation you want to perform:

- UPDATEFQDNLIST - Update the Cisco Cloud Service portal list.
 - FETCHCERTIFICATE - Download the Cisco Talos certificate and key
 - ENABLE_PROXY - Enable connection to Cisco Cloud Server through proxy.
- [> FETCHCERTIFICATE

Current Cisco Talos certificate is valid for 172 days

Do you like to overwrite the existing certificate and key [Y|N] ? [> N

The Content Security Management appliance is successfully registered with the Cisco Cloud Service portal.
Currently used Cisco Cloud Server is api-sse.cisco.com

Example Client Certificate cloudserviceconfig

In the following example, you can use the command to upload the certificate and the key.

```
[> clientcertificate
```

Do you like to overwrite the existing certificate and key [Y|N] ? [> Y

Paste the certificate.
Press CTRL-D on a blank line when done.

```

-----BEGIN CERTIFICATE-----
AQEFAAOCAQ8AMIIBCgKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJ
cVPlrZfWzTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7H0hOYFXcHi95U1Sa
rY6DhYNw8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl80mwl/plErDl5J7MY5kNL
MpES7AmQitef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonF0lrJ
MIIDYzCCAkugAwIBAgIDCMvdMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYDVQQGEwJV
GlyOpFkbHg8ALkdKiD4RHxkUSKdadFDKIAIgc/9g9adrUwIDAQABoxowGDAJBgNV
UZETMBEGA1UECBMkQ2FsaWZvcms5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNV
BAoTEkNpc2NvIFN5c3RlbXMgSW5jLjJERMA8GA1UECXMlU2VjdXJpdHkxGzAZBgNV
BAMTElN0YWdlIEtleW1hc3RlciBDQTAEFw0xOTAyMTkwMzU3MzhaFw0yMjA0MDIw
2jgYEzrhGtZmx+hpAmHili8cnIarD5oePtcggOafxpa/32rqXPGfjiaJU6cdA6Su
Qquqh7/bn6u8R9EMjzu4V+Rn54JZMTCJ9v/u5OC1kKohsMFMwBQ0EpPL5CpM8NDx
SjGPIIMP2SrqtLORlTqtvcx8SnMurrxe61PnrUs93z1nRSXhcHGLyrQs6HIqIvMT
MzU3MzhaMEkxHTAbBgkqhkiG9w0BCQEWdnRlc3RAY2lzy28uY29tMRgwFgYDVQQD
DA9WTE5TTUEXMjM0NTY3ODkxMjM0MjM0MjM0MjM0MjM0MjM0MjM0MjM0MjM0MjM0
AQEFAAOCAQ8AMIIBCgKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJ
cVPlrZfWzTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7H0hOYFXcHi95U1Sa
rY6DhYNw8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl80mwl/plErDl5J7MY5kNL
MpES7AmQitef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonF0lrJ
uT6K+qrTusUEP41oDC7IrpnbBE697xzbtF8l7xgxUosxP+OuXcgtTXlTXcY516jS
GlyOpFkbHg8ALkdKiD4RHxkUSKdadFDKIAIgc/9g9adrUwIDAQABoxowGDAJBgNV
HRMEAjAAMASGA1UdDwQEAwIHGdANBgkqhkiG9w0BAQsFAAOCAQEAOKYfifzJfG4rM
IWM7l3wz8u7Wtj97E6rGVgsj0D54fOKF6DmqHfyqPCuXns0Fl8nL1Da3ogs1LwIrs
d5a11fj/2r6NfbN0hjKN7/5PGBtcRyMDI86aUBoqahNmgCWdKTTJgoVTO0//+Ca
2jgYEzrhGtZmx+hpAmHili8cnIarD5oePtcggOafxpa/32rqXPGfjiaJU6cdA6Su
Qquqh7/bn6u8R9EMjzu4V+Rn54JZMTCJ9v/u5OC1kKohsMFMwBQ0EpPL5CpM8NDx
SjGPIIMP2SrqtLORlTqtvcx8SnMurrxe61PnrUs93z1nRSXhcHGLyrQs6HIqIvMT
JlSwgurFWg==
-----END CERTIFICATE-----
^D

```

Paste Private Key.

Press CTRL-D on a blank line when done.

```

-----BEGIN RSA PRIVATE KEY-----
ZzSwNAdMjtobo6dxliMfbaWd1Um+PIEiBXEY5z74btukQUGTI0DXsCgYEA36q3
gh/+2ybheB8iCYQfZnZkeUM4qqN3HkRmrhTB901PlkZ0B0fstPfpEcw/v/lz3BRQ
Dyk5VlgEtnOpWbyYKqLZbFPHbddQGTIbCV4T1hyEcnByD2SSCIv5gx7F0TBR5qD
14HT3PPT4HXpgcFw70NofNsnNm630hkW4SBNkgCgYEA8Y4VMWA2WWEAFzhIZKS
4Jw8/yWYe4V746aWRVN7wL99aRK6eVtk7kCEZLG7+vmzboSORPi98QXY1o/aBNhg
MIIEowIBAAKCAQEAyf9pD6jCYmA2YUmzjs711J80V2Ehil8FnvDo8ElJcVPlrZfW
NEntal7WnKNZz96nClkaqh8DBaGuoMPTbEGrEjnavfm7JDY/vlLxTUE2SMRd2ZX
zTmI5wHTrQi0YkjaYsbe9Nbh9q5vdmrL58Pmiky7H0hOYFXcHi95U1SarY6DhYNw
BHXHikhk1+8ibEB2K+XlQUPScy7aGmbekc8y0vJBVObdKx+/uIwuk1buy4rUybMy
f3DsaHi6Yj7jYi4aIleC7HT0X60vxc4eahBv8DvaIF3Ak0LyIvdLomycVkg58s1V
Lt+psQKBgfjRVfNddwgC5XQaQXopYJWa/HFnWgH7jXgVFerlQ9smq7L0Yk39GrxT
8isKxFuG0Xnm1mNzSSIQdIcTvqIV/iPUjQl80mwl/plErDl5J7MY5kNLMpES7AmQ
itef0BRmcDmpammCCVmUx2b1A7PmepclCVs2PfaoqIGy26CcAonF0lrJuT6K+qrT
usUEP41oDC7IrpnbBE697xzbtF8l7xgxUosxP+OuXcgtTXlTXcY516jSGLyOpFkb
Hg8ALkdKiD4RHxkUSKdadFDKIAIgc/9g9adrUwIDAQABoIBAE+JQNqJoEmEwSvO
ENgmwcjYE5y3kK+rEt49ALlrs2dAunaZtq1S16TrlXaMzgfJ07/JxDeNxmQlqVL
KaTwwT4BTmvxMqVMdIH6GY0+99ShMT08OxVe3tnXc+m2c8nmX5dftLkcYC5yXNVb
bvtD2BR4eupNOrvj1N5P/+sYcNc4I7ZAAheGfhLc4oDTMIHIE5g6Dyvh7j+Wii9y
bpoU99fFV7jCgtq15AOUQtLUtuO6d1tk2WL1+m2qsX7uMkQ5ddM9vGbTRg0IkjRb
PVPshAK5j/RsQCUN6LlRq+SY7y18Cl1Z4MYWxu754KqMlOk8UDarI+dKISyVskfe
69lNQ2ECgYEA5zLHTykFOA349MyliSXiE6YsVL8tclRyf/PB690oTY+vKUCmCZp
TzLPuEEbyzndAIW7FagV5aYyFXD0kcUE9LUCCT15bToiYJM0YCGgsHnBpqiU7yI
ZzSwNAdMjtobo6dxliMfbaWd1Um+PIEiBXEY5z74btukQUGTI0DXsCgYEA36q3
gh/+2ybheB8iCYQfZnZkeUM4qqN3HkRmrhTB901PlkZ0B0fstPfpEcw/v/lz3BRQ
Dyk5VlgEtnOpWbyYKqLZbFPHbddQGTIbCV4T1hyEcnByD2SSCIv5gx7F0TBR5qD
14HT3PPT4HXpgcFw70NofNsnNm630hkW4SBNkgCgYEA8Y4VMWA2WWEAFzhIZKS
4Jw8/yWYe4V746aWRVN7wL99aRK6eVtk7kCEZLG7+vmzboSORPi98QXY1o/aBNhg
NEntal7WnKNZz96nClkaqh8DBaGuoMPTbEGrEjnavfm7JDY/vlLxTUE2SMRd2ZX
XEDpdHDalZzFpGDrf+wZraECgYB3cTlpe/Dnq43Aji+peUuLdjIvP9Y9Gepk2XZU
BHXHikhk1+8ibEB2K+XlQUPScy7aGmbekc8y0vJBVObdKx+/uIwuk1buy4rUybMy

```

Example: Enabling Cisco SecureX or Cisco Threat Response on Content Security Gateway

```
f3DsaHI6Yj7jYi4aIlec7HT0X60vxc4eahBv8DvaIF3Ak0LyIvdLomycVkg58siV
Lt+psQKBgFjRVfNddwgcX5QaQXopYJWa/HFnWgH7jXgVFeR1Q9smq7L0Yk39GrxT
Gu2acBalPQR474nW9394XqmPTJ5tYhf80nmT7JRwYEgE2C/flnDDea9YFoiX/yP3
fD4kLyDPgQ8utQwK7X7aK1PxdEIsXKZLcR6FoeT0wQj3lgCG2igH
-----END RSA PRIVATE KEY-----
^DCertificate and key are stored successfully
```

Example: Enabling Cisco SecureX or Cisco Threat Response on Content Security Gateway

In the following example, you can use the `cloudserviceconfig > enablesecurex sub` command to enable Cisco SecureX or Cisco Threat Response on your appliance.

Choose the operation you want to perform:

```
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
- SecureX - Configure Cisco SecureX / Threat Response feature on your appliance
[ ]> SecureX
```

The Cisco SecureX / Threat Response feature is currently disabled on your appliance. Would you like to enable Cisco SecureX / Threat Response feature [Y]>

Cloud Service is not enabled.

Enter "cloudserviceconfig" for enabling Cisco Cloud service.

Example: Disabling Cisco SecureX or Cisco Threat Response on Content Security Gateway

In the following example, you can use the `cloudserviceconfig > disablesecurexsub` command to disable Cisco SecureX or Cisco Threat Response on your appliance.

```
sma> generalconfig
```

Choose the operation you want to perform:

```
- IEOVERRIDE - Configure Internet Explorer Compatibility Mode Override
- SecureX - Configure Cisco SecureX / Threat Response feature on your appliance
[ ]> SecureX
```

The Cisco SecureX / Threat Response feature is currently enabled on your appliance. Would you like to disable Cisco SecureX / Threat Response feature [N]> Y

The Cisco SecureX / Threat Response feature is currently disabled on your appliance. The Cisco Cloud Service is currently disabled on your appliance.

updateconfig

- [Description, on page 464](#)
- [Usage, on page 464](#)
- [Example: Uploading Cisco Talos Certificate and Key Details in Secure Email and Web Manager, on page 465](#)
- [Example: Configuring Secure Email and Web Manager to Add or Update VLNID, on page 466](#)

Description

Configure system update parameters.

Usage

Commit: This command requires a 'commit'.

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



Note The `CLIENTCERTIFICATE` and `VLNID` subcommands do not require a ‘commit’.



Note The `VLNID` subcommand is only applicable for SLR or PLR registered virtual devices (that is, SLR or PLR registered device operating in air-gap mode).

Example: Uploading Cisco Talos Certificate and Key Details in Secure Email and Web Manager

```
mail.example.com> updateconfig
Service (images):                               Update URL:
-----
Feature Key updates                             http://downloads.ironport.com/asyncos
Timezone rules                                 Cisco Servers
Support Request updates                       Cisco Servers
Smart License Agent Updates                  Cisco Servers
Notifications component Updates             Cisco Servers
Cisco AsyncOS upgrades                      Cisco Servers

Service (list):                                Update URL:
-----
Timezone rules                                 Cisco Servers
Support Request updates                       Cisco Servers
Smart License Agent Updates                  Cisco Servers
Notifications component Updates             Cisco Servers
Cisco AsyncOS upgrades                      Cisco Servers

Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VLNID - Update the VLN ID.
[ ]> CLIENTCERTIFICATE

Paste the certificate.
Press CTRL-D on a blank line when done.

-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIEAm+eGTANBgkqhkiG9w0BAQsFADB+MQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvcn5pYTERMA8GA1UEBwwIU2FuIEpvc2UxGzAZBgNV
BAoMEkNpc2NvIFN5c3RlbXMgSW5jLjJERMA8GA1UECwwIU2VjdxJpdHkxZzAVBgNV
.....
GONYIhd82O9NIP9WQeVJmPfd402EFZZQb6Mq+EvkCYajTWInUfxQLIfy3HUEDGJ
ZKY=
-----END CERTIFICATE-----
^D

Paste Private Key.
Press CTRL-D on a blank line when done.
Key      :

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAttALQE31Pd+xoLaO8kpzjHBuoJVRsZnNbt400PRES8vXSsYS
bxU720rK9xPTdYQ1V9bJULPvYHlgIE90xPcWfnptUsARFTrvnsMGydI3J+5vD9gN
5Y9LjWlrmNUWdF98022hEzJpZ35nUT6EePd8uOlw7MmMopSF4ySrG5imseMr6fBI
```

Example: Configuring Secure Email and Web Manager to Add or Update VLNID

```
.....
VBgX7nSeTCXsSZdpvTi7RIk+jCEYqeZVGWJ4tZF6yZWIOaTTCFw=
-----END RSA PRIVATE KEY-----
^D
Certificate and key are stored successfully
```

Example: Configuring Secure Email and Web Manager to Add or Update VLNID

```
mail.example.com> updateconfig
Service (images):                Update URL:
-----
Feature Key updates              http://downloads.ironport.com/asyncos
Timezone rules                   Cisco Servers
Support Request updates          Cisco Servers
Smart License Agent Updates      Cisco Servers
Notifications component Updates  Cisco Servers
Cisco AsyncOS upgrades          Cisco Servers

Service (list):                  Update URL:
-----
Timezone rules                   Cisco Servers
Support Request updates          Cisco Servers
Smart License Agent Updates      Cisco Servers
Notifications component Updates  Cisco Servers
Cisco AsyncOS upgrades          Cisco Servers

Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VLNID - Update the VLN ID.

[ ]> VLNID

VLN : VLNESA1838283016
Do you like to overwrite the existing VLN[Y|N] ? [ ]> n
```

vlinfo

- [Description, on page 466](#)
- [Usage, on page 466](#)
- [Example: Displaying VLN and Cisco Talos Certificate and Key Details, on page 467](#)

Description

Display the Virtual License Number (VLN), and Cisco Talos Certificate and Key details.

Usage

Commit: This command does not require a ‘commit’.

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



Note The `vlinfo` command is only applicable for Smart Software Licensing registered and SLR or PLR registered virtual devices.

Example: Displaying VLN and Cisco Talos Certificate and Key Details

```
mail.example.com> vlinfo

VLN and Certificate details

VLN          : VLNSMA1838285196

Certificate :

-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIEAm+eGTANBgkqhkiG9w0BAQsFAADB+MQswCQYDVQQGEwJV
UzETMBEGA1UECAwKQ2FsaWZvc5pYTERMA8GA1UEBwwIU2FuIEpvc2UxGzAZBgNV
BAoMEkNpc2NvIFN5c3RlbXMgSW5jLjJERMA8GA1UECwwIU2VjdXJpdHkxZzAVBgNV
.....
G0NYIhd8209NIP9WQeVJmPftd402EFZZQb6Mq+EvkCYajTWInUfxQLIfy3HUEDGJ
ZKY=
-----END CERTIFICATE-----

Key          :

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAttALQE31Pd+xoLaO8kpzjHBuoJVRsZnNbt400PRES8vXSsYS
bxU720rk9xPTdYQ1V9bJUlPvYHlgIE90xPcWfnptUsARFTrvnsMGydI3J+5vD9gN
5Y9LjWlrmNUwdf98022hEzJpZ35nUT6EePd8uO1w7MmMopSF4ySrG5imseMr6fBI
.....
VBgX7nSeTCXsSZdpvTi7RIk+jCEYqeZVGWJ4tZf6yZWIOaTTCFw=
-----END RSA PRIVATE KEY-----
```

help vlinfo

- [Description, on page 467](#)
- [Usage, on page 467](#)
- [Example: Displaying VLN details, on page 468](#)

Description

Display the VLN details. It provides the help support for `vlinfo` command.

Usage

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

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



Note The `help vlinfo` command is only applicable for Smart Software Licensing registered and SLR or PLR registered virtual devices.

Example: Displaying VLN details

```
mail.example.com> help vlninfo
```

```
Show VLN details
```

Smart Software Licensing Key Points for AsyncOS 14.0

- Cisco SecureX will be automatically enabled when you enable Cloud Services and Cisco SecureX will be disabled when Cloud Services is disabled.
- Cisco SecureX and Cisco Threat Response option is now changed in the Web UI and you can enable or disable Cisco SecureX and Cisco Threat Response from **System Administration > General Settings**. You can also perform the same from CLI by using the **generalconfig** command.
- Cloud Service will be enabled and Appliance (security services exchange) will be registered automatically when smart software licensing is enabled and registered.
- In Classic Mode, Cloud Service will be in disabled state by default. You need to enable it manually and Cisco SecureX and Cisco Threat Response will be enabled. You must enable smart licensing mode for auto-registration to occur.
- After Enabling Smart Software Licensing, the Smart Agent is started and once the registration is completed, Cloud services will be enabled.
- You cannot perform an security services exchange auto registration when smart license is with evaluation mode.

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
- suspendtransfers
- resume
- resumetransfers
- resetconfig
- version

Shutting Down the Security Management Appliance

To shut down your Security Management appliance, do the following:

- 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.

Taking the Security Management Appliance Out of Service

If you want to take the appliance offline, for example to perform system maintenance, use one of the following commands:

Command	Description	Persistence
<code>suspend</code>	<ul style="list-style-type: none"> • Suspends transfer of quarantined messages from the Email Security appliance to the Security Management appliance. • Suspends delivery of messages released from quarantines. • Inbound email connections are not accepted. • Outbound email delivery is halted. • Log transfers are halted. • The CLI remains accessible. 	Persists after reboot.
<code>suspendtransfers</code>	<p>Suspends transfer of reporting and tracking data from managed email and web security appliances to the content security management appliance.</p> <p>This command also suspends receiving of quarantined messages from Email Security appliances.</p> <p>Use this command when preparing to bring a backup appliance into service as the primary appliance.</p>	Persists after reboot.

You must enter a delay for the appliance when using these commands. 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, service is suspended immediately.

To re-activate services that were halted by the `suspend` or `suspendtransfers` commands, use the `resume` or `resumetransfers` commands, respectively.

To determine the current online/suspended status of the management appliance, select **Management Appliance > System Administration > Shutdown/Reboot** in the web interface.

See also:

- “Suspending Email Delivery,” “Resuming Email Delivery,” “Suspending Receiving,” and “Resuming Receiving” in the documentation or online help for your Email Security appliance.

CLI Examples: suspend and suspendtransfers Commands

```
sma.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.
sma.example.com>
sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

Resuming from a Suspended State

The resume command returns the appliance to normal operating state after using the suspend or suspenddel command.

The resumetransfers command returns the appliance to normal operating state after using the suspendtransfers command.

CLI Examples: resume and resumetransfers Commands

```
sma.example.com> resume
Receiving resumed.
Mail delivery resumed.
sma.example.com>
sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.example.com>
```

Resetting the Configuration to Factory Defaults

When physically transferring the appliance, or as a last resort for solving configuration issues, you may want to reset the appliance to factory defaults.



Caution

Resetting the configuration will disconnect you from the CLI, disable services that you used to connect to the appliance (FTP, Telnet, SSH, HTTP, HTTPS), and remove user accounts.

To	Do This
<ul style="list-style-type: none"> Reset all configurations to factory defaults Clear all reporting counters <p>But</p> <ul style="list-style-type: none"> Retain log files Retain quarantined messages 	<ol style="list-style-type: none"> Ensure that you can connect to the appliance after reset using the default admin user account and passphrase, either to the CLI using the serial interface or to the Management port using the default settings. See chapter Setup, Installation, and Basic Configuration, on page 7 for information about accessing an appliance having default settings. Suspend service on the appliance. Select Management Appliance > System Administration > Configuration File and click Reset. <p>Note After resetting, the appliance automatically returns to the online state. If mail delivery was suspended before reset, delivery will be attempted again after the reset.</p>
<ul style="list-style-type: none"> Reset all configurations to factory defaults Remove all data 	<p>Use the <code>diagnostic > reload</code> CLI command.</p> <p>Caution This command is NOT the same as the similar command used on a Cisco router or switch.</p>

Resetconfig CLI Command

```
mail3.example.com> suspend
Delay (seconds, minimum 30):
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com> resetconfig
Are you sure you want to reset all configuration values? [N]> Y
All settings have been restored to the factory default.
```

Diagnostic - Reload Subcommand

The `Diagnostic - Reload` subcommand resets the configuration to the initial manufacturer values. This subcommand removes all user settings and resets the entire device.

If the Secure Email and Web Manager is a virtual appliance, then the `Diagnostic - Reload` subcommand will remove all the feature keys, and you must load the license again.



Note You may lose connection to the device if you are remotely connected to the system.

```
mail3.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
```

```

- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[ ]> reload
This command will remove all user settings and reset the entire device.

```

```

If this is a Virtual Appliance, all feature keys will be removed, and the license must be
reapplied. This resets network configuration to factory defaults. You might lose connection
to the device if you are connected remotely.
Are you sure you want to continue? [N]> Y
Are you *really* sure you want to continue? [N]> Y
Do you want to wipe also? Warning: This action is recommended if the device is being sanitized
before sending it for RMA. Sometimes, it may take several minutes to complete the process
because it follows the NIST Purge standard.
Do you want to continue? [N]

```

Diagnostic - Reload Status Command

The `Diagnostic - Reload_Status` subcommand displays the status of the execution of the last `Diagnostic - Reload` command.


```

mail3.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[ ]> reload_status

Last Reload Status      Last Updated
Successful              09 Feb 2023 09:12 (GMT)

```

Displaying the Version Information for AsyncOS

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliances > Centralized Services > System Status**.
- Step 3** 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.
-

Enabling Remote Power Cycling

The ability to remotely reset the power for the appliance chassis is available only on 80- and 90- series hardware.

If you want to be able to remotely reset appliance power, you must enable and configure this functionality in advance, using the procedure described in this section.

Before you begin

- Cable the dedicated Remote Power Cycle (RPC) port directly to a secure network. For information, see hardware documentation for your model, available from the location listed in [Documentation](#) , on page 629.
- Ensure that the appliance is accessible remotely; for example, open any necessary ports through the firewall.
- This feature requires a unique IPv4 address for the dedicated Remote Power Cycle interface. This interface is configurable only via the procedure described in this section; it cannot be configured using the `ipconfig` command.
- In order to cycle appliance power, you will need a third-party tool that can manage devices that support the Intelligent Platform Management Interface (IPMI) version 2.0. Ensure that you are prepared to use such a tool.
- For more information about accessing the command-line interface, see the CLI reference guide.

Step 1 Use SSH, telnet, or the serial console port to access the command-line interface.

Step 2 Sign in using an account with Administrator access.

Step 3 Enter the following commands:

```
remotepower
setup
```

Step 4 Follow the prompts to specify the following:

- The dedicated IP address for this feature, plus netmask and gateway.
- The username and passphrase required to execute the power-cycle command.

These credentials are independent of other credentials used to access your appliance.

Step 5 Enter `commit` to save your changes.

Step 6 Test your configuration to be sure that you can remotely manage appliance power.

Step 7 Ensure that the credentials that you entered will be available to you in the indefinite future. For example, store this information in a safe place and ensure that administrators who may need to perform this task have access to the required credentials.

What to do next

[Remotely Resetting Appliance Power](#) , on page 607

Monitoring System Health Using SNMP

AsyncOS supports system status monitoring via Simple Network Management Protocol (SNMP) versions v1, v2, and v3.

- To enable and configure SNMP, use the `snmpconfig` command in the command-line interface.
- MIBs are available from <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html> use the latest available files.
- The use of SNMPv3 with passphrase authentication and DES Encryption is mandatory to enable this service. (For more information on SNMPv3, see RFCs 2571-2575.) You are required to set a SNMPv3 passphrase of at least 8 characters to enable SNMP system status monitoring. The first time you enter a SNMPv3 passphrase, you must re-enter it to confirm. The `snmpconfig` command “remembers” this phrase the next time you run the command.

- When setting up SNMP to monitor connectivity:

When entering the `url-attribute` while configuring a `connectivityFailure` SNMP trap, determine whether the URL is pointing at a directory or a file.

- If it is a directory, add a trailing slash (/)
 - If it is a file, do not add a trailing slash
- Additional information about using SNMP with AsyncOS is available in the online help for your web or email security appliance.

Example: snmpconfig Command

```
sma.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[ ]> SETUP
Do you want to enable SNMP?
[Y]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: sma.example.com)
[1]>
Which port shall the SNMP daemon listen on interface "Management"?
[161]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2
Enter the SNMPv3 authentication passphrase.
[ ]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[ ]>
```



```
Enter the SNMPv3 privacy passphrase.
[ ]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[ ]>
Service SNMP V1/V2c requests?
[ N ]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[ Y ]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded      Disabled
2. FIPSMoDeDisableFailure      Enabled
3. FIPSMoDeEnableFailure       Enabled
4. FailoverHealthy             Enabled
5. FailoverUnhealthy           Enabled
6. RAIDStatusChange            Enabled
7. connectivityFailure         Disabled
8. fanFailure                   Enabled
9. highTemperature             Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded  Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[ N ]> Y
Do you want to disable any of these traps?
[ Y ]> n
Do you want to enable any of these traps?
[ Y ]> y
Enter number or numbers of traps to enable. Separate multiple numbers with
commas.
[ ]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> SMA.Administrator@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: SMA.Administrator@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[ ]>
```

```
sma.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
sma.example.com>
```

Backing Up Security Management Appliance Data

- [What Data Is Backed Up](#) , on page 476
- [Restrictions and Requirements for Backups](#) , on page 476
- [Backup Duration](#) , on page 478
- [Availability of Services During Backups](#) , on page 478
- [Interruption of a Backup Process](#) , on page 478
- [Prevent the Target Appliance From Pulling Data Directly from Managed Appliances](#) , on page 479
- [Receiving Alerts About Backup Status](#) , on page 479
- [Scheduling Single or Recurring Backups](#), on page 479
- [Starting an Immediate Backup](#), on page 480
- [Checking Backup Status](#) , on page 480
- [Other Important Backup Tasks](#) , on page 481
- [Making a Backup Appliance the Primary Appliance](#) , on page 481

What Data Is Backed Up

You can choose to back up all data, or any combination of the following data:

- Spam quarantine, including messages and meta data
- Centralized policy, virus, and outbreak quarantines, including messages and meta data
- Email tracking (message tracking), including messages and meta data
- Web tracking
- Reporting (Email and Web)
- Safelist/blocklist

After the data transfer is finished, the data on the two appliances will be identical.

Configurations and logs are not backed up using this process. To back up those items, see [Other Important Backup Tasks](#) , on page 481.

Each backup after the first backup copies only the information generated since the last backup.

Restrictions and Requirements for Backups

Be sure to address the following restrictions and requirements before you schedule a backup:

Restriction	Requirement
AsyncOS version	The AsyncOS version of the source and target Security Management appliances must be the same. If there is a version incompatibility, upgrade appliances to the same release before scheduling a backup.
Target appliance on the network	The target appliance must be set up on the network. If the target appliance is new, run the System Setup Wizard to enter the necessary information. For instructions, see Setup, Installation, and Basic Configuration, on page 7
Communication between source and target appliances	The source and target Security Management appliances must be able to communicate using SSH. Therefore: <ul style="list-style-type: none"> • Port 22 must be open on both appliances. By default, this port is opened when you run the System Setup Wizard. • The Domain Name Server (DNS) must be able to resolve the host names of both appliances using both A records and PTR records.
Target appliance must not be in service	Only the primary appliance should pull data from managed email and web security appliances. To ensure this, see Prevent the Target Appliance From Pulling Data Directly from Managed Appliances , on page 479. Also, cancel any scheduled configuration publishing jobs on the backup appliance.
Appliance capacity	The disk space capacity of the target appliance must be the same as or greater than the capacity of the source appliance. Disk space allocated to each type of data (reporting, tracking, quarantine, etc.) on the target appliance cannot be less than the corresponding allocation on the source appliance. You can schedule a backup from a larger source to a smaller target Security Management appliance as long as there is enough space on the target appliance for all of the data being backed up, for each type of data. If the source appliance is larger than the target appliance, you must reduce the space allocated on the source appliance to match the space available on the smaller target appliance. To view and manage disk space allocations and capacity, see Managing Disk Space , on page 521. For disk capacity of virtual appliances, see the <i>Cisco Content Security Virtual Appliance Installation Guide</i> .
Multiple, concurrent, and chained backups	Only one backup process can run at a time; a backup that is scheduled to run before a previous backup has been completed will be skipped and a warning sent. Data from a Security Management appliance can be backed up to a single Security Management appliance. Chained backup (a backup to a backup) is not supported.

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

Backing up a Security Management appliance copies the active data set from the ‘source’ Security Management appliance to a ‘target’ Security Management appliance with minimum disruption on the originating ‘source’ appliance.

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 services on both the source and the target appliances are returned to the state they were in when backup was initiated. 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 at the top of the page that a system backup is in progress.

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.

Canceling a backup in progress is not recommended, as the existing data will be incomplete and may not be usable until a subsequent backup is completed, especially if you receive an error. If you must cancel a backup in progress, be sure to run a complete backup as soon as possible to ensure that you always have a usable current backup.

Prevent the Target Appliance From Pulling Data Directly from Managed Appliances

-
- Step 1** Access the command-line interface of the target appliance. For instructions, see [Accessing the Command Line Interface, on page 14](#).
- Step 2** Run the `suspendtransfers` command.
- Step 3** Wait for the prompt to reappear.
- Step 4** Run the `suspend` command.
- Step 5** Wait for the prompt to reappear.
- Step 6** Exit the command-line interface of the target appliance.
-

Receiving Alerts About Backup Status

To receive alerts when backups are complete and be informed of any issues, configure the appliance to send you alerts of type System, severity Info. See [Managing Alerts, on page 499](#).

Scheduling Single or Recurring Backups

You can schedule a single or recurring backup to occur at a predetermined time.



Note A backup process will not start if there are any ongoing backups on the remote machine.

Before you begin

- Address the items in [Restrictions and Requirements for Backups , on page 476](#).
- Make sure you disable two-factor authentication temporarily on the target appliance before you begin the backup process. Once the backup process is complete, you can enable two-factor authentication on the target appliance.

-
- Step 1** Login, as administrator, to the command-line interface of the source appliance.
- Step 2** At the command prompt, type `backupconfig` and press **Enter**.
- Step 3** If the connection between source and target appliances is slow, turn on data compression:
Type `setup` and enter **Y**.
- Step 4** Type `Schedule` and press **Enter**.
- Step 5** Type the IP address of the target Security Management appliance.
- Step 6** Enter a meaningful name to identify the target appliance (up to 20 characters).
- Step 7** Enter the admin user name and passphrase for the target appliance.
- Step 8** Respond to prompts about which data you want to back up.

- Step 9** To schedule a single backup, type **2** to Schedule a single backup and press **Enter**.
- Step 10** To schedule a recurring backup:
- Type **1** to Setup Repeating Backup Schedule and press **Enter**.
 - Choose the frequency for your periodic backup and press **Enter**.
- Step 11** Type the specific date or day and time that you want the backup to start and press **Enter**.
- Step 12** Type the name of the backup process.
- Step 13** Verify that the backup was successfully scheduled: Type **View** and press **Enter** at the command prompt.
- Step 14** See also [Other Important Backup Tasks](#) , on page 481.

Starting an Immediate Backup



Note A backup process will not start if there are any ongoing backups on the target machine.

Before you begin

Meet all requirements in [Restrictions and Requirements for Backups](#) , on page 476.

- Step 1** Login, as administrator, to the command-line interface of the source appliance.
- Step 2** At the command prompt, type `backupconfig` and press **Enter**.
- Step 3** If the connection between source and target appliances is slow, turn on data compression:
Type `setup` and enter **Y**.
- Step 4** Type **Schedule** and press **Enter**.
- Step 5** Type the IP address of the target Security Management appliance.
- Step 6** Enter a meaningful name to identify the target appliance (up to 20 characters).
- Step 7** Enter the admin user name and passphrase for the target appliance.
- Step 8** Respond to prompts about which data you want to back up.
- Step 9** Type **3** to Start a Single Backup Now and press **Enter**.
- Step 10** Enter a meaningful name for the backup job.
The backup process begins in a few minutes.
- Step 11** (Optional) To see the progress of the backup, type **Status** at the command-line prompt.
- Step 12** See also [Other Important Backup Tasks](#) , on page 481.

Checking Backup Status

- Step 1** Log in, as administrator, to the command-line interface of the primary appliance.

Step 2 At the command prompt, type **backupconfig** and press **Enter**.

To Check Status Of	Do This
A scheduled backup	Choose the View operation.
A backup in progress	Choose the Status operation. If you have configured alerts, check your email or see Viewing Recent Alerts , on page 501.

What to do next

Related Topics

[Backup Information in Log Files](#) , on page 481

Backup Information in Log Files

Backup logs record the backup process from start to finish.

Information about backup scheduling is in the SMA logs.

Related Topics

- [Checking Backup Status](#) , on page 480

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, and to speed setup of your replacement Security Management appliance in case of appliance failure:

- To save the settings from your primary Security Management appliance, see [Saving and Importing Configuration Settings](#) , on page 513. Save the configuration file to a safe location separate from your primary Security Management appliance.
- Save any Web Security appliance configuration files that you used to populate your Configuration Masters.
- To save log files from your Security Management appliance to an alternate location, see [Log Subscriptions](#), on page 591.


Additionally, you can set up a log subscription for Backup Logs. See [Creating a Log Subscription in the GUI](#), on page 593.

Making a Backup Appliance the Primary Appliance

If you are upgrading appliance hardware, or if you need to switch appliances for any other reason, use this procedure.

Before you begin

Review the information in [Backing Up Security Management Appliance Data](#) , on page 476.

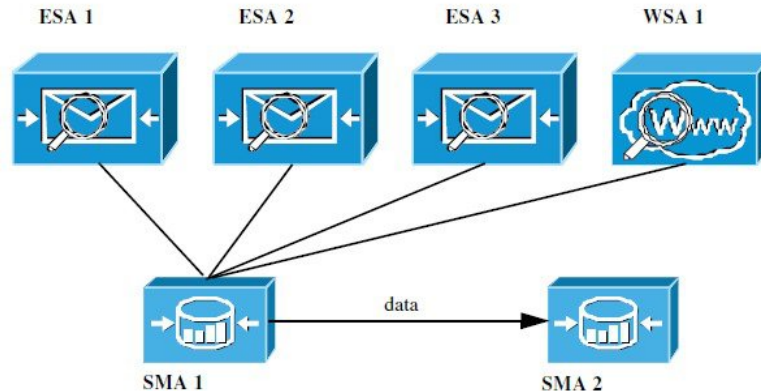
-
- Step 1** Save a copy of the configuration file from your old/primary/source appliance to a location that you can reach from the new appliance. See [Saving and Importing Configuration Settings](#), on page 513.
- Step 2** Run the System Setup Wizard on the new/backup/target appliance.
- Step 3** Meet the requirements in [Restrictions and Requirements for Backups](#), on page 476.
- Step 4** Run a backup from the old/primary/source appliance. See instructions at [Starting an Immediate Backup](#), on page 480.
- Step 5** Wait for the backup to complete.
- Step 6** Run the suspendtransfers and suspend commands on the old/primary/source appliance.
- Step 7** Run a second backup to transfer last-minute data from the old/primary/source to the new/backup/target appliance.
- Step 8** Import the configuration file into the new/backup/target appliance.
- Step 9** Run the resumetransfers and resume commands on the new/backup/target appliance.
Do NOT run this command on the old/original primary/source appliance.
- Step 10** Establish the connection between the new/backup/target appliance and the managed email and web security appliances:
- Step 11**
- [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Select **Management Appliance > Centralized Services > Security Appliances**.
 - Click an appliance name.
 - Click the **Establish Connection** button.
 - Click **Test Connection**.
 - Return to the list of appliances.
 - Repeat for each managed appliance.
- Step 12** Verify that the new/target appliance is now functioning as the primary appliance:
Select **Management Appliance > Centralized Services > System Status** and check the status of data transfers.
-

Disaster Recovery on the Security Management Appliance

If your Security Management appliance unexpectedly fails, use the following procedure to restore security management services and your backed-up data, which you regularly save using the information in [Backing Up Security Management Appliance Data](#), on page 476.

A typical appliance configuration might look as shown in the following figure:

Figure 14: Disaster Recovery: A Typical Environment



In this environment, SMA 1 is the primary Security Management appliance that is receiving data from ESAs 1-3 and WSA 1. SMA 2 is the backup Security Management appliance receiving backup data from SMA1.

In case of failure, you must configure SMA 2 to be your primary Security Management appliance.

To configure SMA 2 as your new primary Security Management appliance and restore service:

Procedure

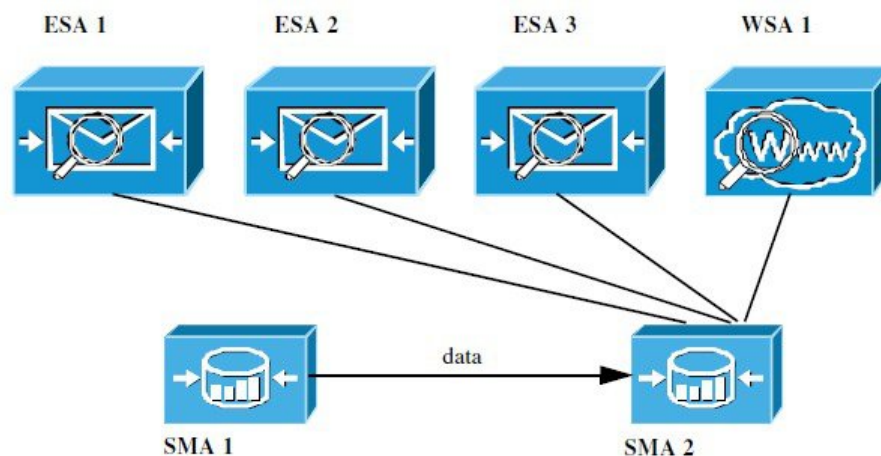
	Command or Action	Purpose
Step 1	If you are using Centralized Policy, Virus, and Outbreak Quarantines: <ul style="list-style-type: none"> On each Email Security appliance, disable the centralized quarantines. 	See instructions for disabling Centralized Policy, Virus, and Outbreak Quarantines in the Email Security appliance documentation. This will create local quarantines on each Email Security appliance, which you will migrate later to the new Security Management appliance.
Step 2	Load onto your backup Security Management appliance (SMA2) the configuration file that you saved from your primary Security Management appliance (SMA1).	See Loading a Configuration File, on page 514 .
Step 3	Recreate the IP address from the failed SMA 1 to be the IP address on SMA 2	a. On SMA 2 choose Network > IP Interfaces > Add IP Interfaces . b. 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 about Adding IP Interfaces, see Configuring IP Interfaces, on page 610 .
Step 4	Submit and commit your changes.	
Step 5	Enable all applicable centralized services on the new Security Management appliance (SMA 2).	See Configuring Services on the Security Management Appliance, on page 20 .
Step 6	Add all appliances on to the new Security Management appliance (SMA 2).	See About Adding Managed Appliances, on page 19 .

	Command or Action	Purpose
	<ul style="list-style-type: none"> • Test to see that each appliance is enabled and working by establishing a connection to the appliances and testing the connections. 	
Step 7	If you are using Centralized Policy, Virus, and Outbreak Quarantines, configure quarantine migration on the new Security Management appliance, then enable and configure the migration on each applicable Email Security appliance.	See Centralizing Policy, Virus, and Outbreak Quarantines , on page 305.
Step 8	If necessary, restore additional data.	See Other Important Backup Tasks , on page 481.

What to do next

After this process is complete, SMA 2 becomes the primary Security Management appliance. All data from ESAs 1-3 and WSA 1 now goes to SMA 2, as shown in the following figure:

Figure 15: Disaster Recovery: Final Result



Upgrading Appliance Hardware

See [Making a Backup Appliance the Primary Appliance](#) , on page 481.

Upgrading AsyncOS

- [Batch Commands for Upgrades](#) , on page 485
- [Determining Network Requirements for Upgrades and Updates](#) , on page 485
- [Choosing an Upgrade Method: Remote vs. Streaming](#) , on page 485
- [Configuring Upgrade and Service Update Settings](#) , on page 487
- [Before You Upgrade: Important Steps](#) , on page 492
- [Upgrading AsyncOS](#) , on page 484
- [Viewing Status of, Canceling, or Deleting a Background Download](#) , on page 494

- [After Upgrading](#) , on page 495

Batch Commands for Upgrades

Batch commands for upgrade procedures are documented in the CLI Reference Guide for AsyncOS for Email at <http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html>

Determining Network Requirements for Upgrades and Updates

The update servers for Cisco content security appliances 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 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.

Choosing an Upgrade Method: Remote vs. Streaming

Cisco provides two methods (or ‘sources’) for upgrading AsyncOS on your appliances:

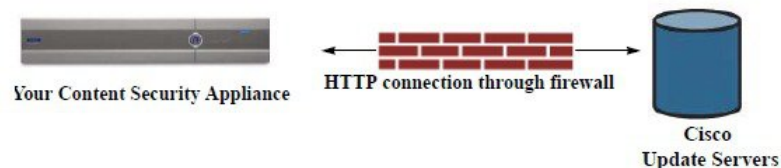
- Streaming upgrades — Each appliance downloads the AsyncOS upgrades via HTTP directly from the Cisco content security update servers.
- Remote upgrades — You only download the upgrade image from Cisco one time, and then serve it to your appliances. Your appliances then download the AsyncOS upgrades from a server within your network.

You will configure the upgrade method in [Configuring Upgrade and Service Update Settings](#), on page 487. Optionally, use the `updateconfig` command in the CLI.

Streaming Upgrade Overview

In Streaming upgrades, each Cisco Content Security appliance connects directly to the Cisco content security update servers to find and download upgrades:

Figure 16: Streaming Update Method

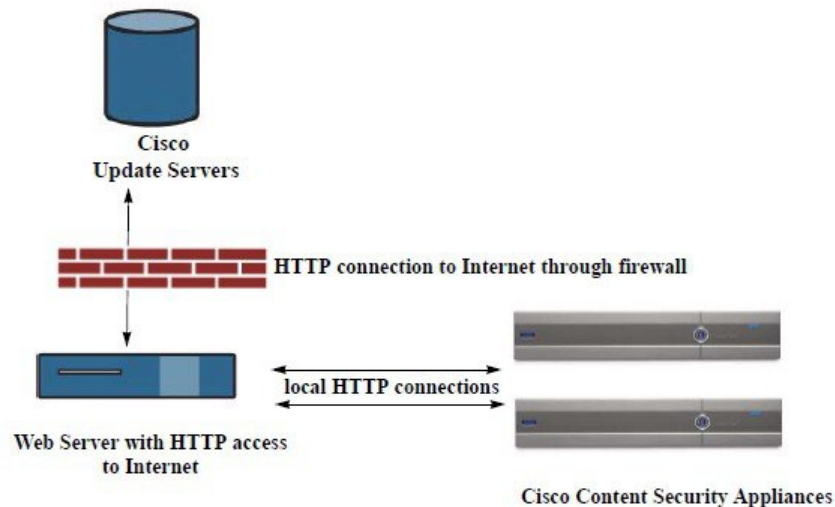


This method requires that your appliance contacts the Cisco content security update servers directly from the network.


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 the Cisco 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 Security Management appliances.

Figure 17: Remote Update Method



The basic process is as follows:

-
- Step 1** Read the information in [Hardware and Software Requirements for Remote Upgrades, on page 486](#) and [Hosting a Remote Upgrade Image, on page 487](#).
 - Step 2** Configure a local server to retrieve and serve the upgrade files.
 - Step 3** Download the upgrade files.
 - Step 4** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 5** Choose **Management Appliance > System Administration > Update Settings**
From this page, choose to configure the appliance to use the local server.
 - Step 6** Choose **Management Appliance > System Administration > System Upgrade**
 - Step 7** Click **Available Upgrades**.

Note From the command-line prompt you can also do the following: Run the **updateconfig** command then run the **upgrade** command.

For complete information, see [Upgrading AsyncOS, on page 484](#).

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 update servers for Cisco content security appliances.
- 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 to download a zip file of an upgrade image. To download the image, enter your serial number and the version number of the Cisco Content Security 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 Content Security appliances on your network to the version selected at http://updates.ironport.com/fetch_manifest.html. Your Cisco Content Security appliances still download the upgrade from the Cisco servers. If you want to host the upgrade list on a local server, download the zip file and extract the `asyncoos/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, check the Knowledge Base (see [Knowledge Base Articles \(TechNotes\)](#), on page 631) or contact your support provider.

Important Differences in Remote Upgrading Method

Note these differences when upgrading AsyncOS from a local server (Remote upgrade) as opposed to the Streaming upgrade method:

- The upgrade 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 Cisco Content Security appliance downloads security services updates (such as time zone rules) and AsyncOS upgrades. For example, you can choose whether to download upgrades and updates dynamically from Cisco servers or from a local server onto which you have made the images available; 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 in the GUI (see the following two sections) or using the `updateconfig` command in the CLI.

You can also configure upgrade notification settings.

Upgrade and Update Settings

The following table describes the update and upgrade settings you can configure.

Table 83: Update Settings for Security Services

Setting	Description
Update Servers (images)	<p>Choose whether to download AsyncOS upgrade and service update software images, such as time zone rules and Feature Key updates, from the Cisco servers or a from a local web server. The default is the Cisco servers for both upgrades and updates.</p> <p>You might want to use a local web server if :</p> <ul style="list-style-type: none"> • You need to download images to your appliance from a static address. See Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies , on page 489. • You want to download AsyncOS upgrade images to your appliance at your convenience. (You can still download service update images dynamically from the Cisco update servers.) <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 passphrase.</p> <p>For more information, see Choosing an Upgrade Method: Remote vs. Streaming , on page 485 and Remote Upgrade Overview, on page 486.</p>
Update Servers (lists)	<p>Choose whether to download the lists of available upgrades and service updates (the manifest XML files) from the Cisco servers or from a local web server.</p> <p>The default for both upgrades and updates is the Cisco servers. You can choose different settings for upgrades and for updates.</p> <p>If applicable, see Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies , on page 489.</p> <p>If you choose local update servers, enter the full path to the manifest XML file for each 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 passphrase.</p> <p>For more information, see Choosing an Upgrade Method: Remote vs. Streaming , on page 485 and Remote Upgrade Overview, on page 486.</p>
Automatic Updates	<p>Choose whether or not to enable automatic updates for time zone rules. When enabled, enter the time to wait between checks for updates. Add a trailing m for minutes, h for hours, and d for days.</p>

Setting	Description
Interface	Choose which network interface to use when contacting the update servers for time zone rules and AsyncOS upgrades. The available proxy data interfaces are shown. By default, the appliance selects an interface to use.
HTTP Proxy Server	<p>If an upstream HTTP proxy server exists and requires authentication, enter the server information and user name and passphrase here.</p> <p>Note that if you specify a proxy server, it will be used to access and update the services listed in the GUI.</p> <p>This proxy server is also used to obtain File Analysis report details from the cloud. See also Requirements for File Analysis Report Details , on page 82 (Web reports) or Requirements for File Analysis Report Details , on page 183 (Email reports).</p>
HTTPS Proxy Server	<p>If an upstream HTTPS proxy server exists and requires authentication, enter the server information and user name and passphrase here.</p> <p>Note that if you specify a proxy server, it will be used to access and update the services listed in the GUI.</p> <p>This proxy server is also used to obtain File Analysis report details from the cloud.. See also Requirements for File Analysis Report Details , on page 82 (Web reports) or Requirements for File Analysis Report Details , on page 183 (Email reports).</p>

Static Upgrade and Update Server Settings for Environments with Strict Firewall Policies

The AsyncOS update servers use dynamic IP addresses. If your environment has strict firewall policies which require static IP addresses, use the following settings on the Update Settings page:

Figure 18: Static URLs for Update Servers (images) Settings

Update Servers (images): *The update servers will be used to obtain **update images** for the following services:*

- Feature Key updates
- Time zone rules
- Cisco IronPort AsyncOS upgrades

Cisco IronPort Update Servers

Local Update Servers (location of update image files)

Base Url (all services except Time zone rules and Cisco IronPort AsyncOS upgrades): Port:
http://downloads.example.com

Authentication (optional):

Username:

Password:

Retype Password:

Base Url (Time zone rules):
format: downloads.example.com:80

▼ Click to use different settings for AsyncOS upgrades:

AsyncOS Upgrade settings

Cisco IronPort Update Servers

Local Update Servers (location of update image files)

Host (Cisco IronPort AsyncOS upgrades): Port: (optional)
Ex. downloads.example.com

Figure 19: Static URLs for Update Servers (list) Settings

Update Servers (list):	The URL will be used to obtain the list of available updates for the following services: - Time zone rules	
	<input type="radio"/> Cisco IronPort Update Servers <input checked="" type="radio"/> Local Update Servers (location of list of available updates file)	
	Full Url	<input type="text" value="http://update-manifests.ironport.com"/> Port: <input type="text" value="443"/> <input type="text" value="http://updates.example.com/my_updates.xml"/>
	Authentication (optional):	
	Username: <input type="text"/>	
	Password: <input type="text"/>	
	Retype Password: <input type="text"/>	
	The URL will be used to obtain the list of available updates for the following services: - Cisco IronPort AsyncOS upgrades	
	<input type="radio"/> Cisco IronPort Update Servers <input checked="" type="radio"/> Local Update Servers (location of list of available updates file)	
	Full Url	<input type="text" value="http://update-manifests.ironport.com"/> Port: <input type="text" value="443"/> <input type="text" value="http://updates.example.com/my_updates.xml"/>
	Authentication (optional):	
	Username: <input type="text"/>	
	Password: <input type="text"/>	
	Retype Password: <input type="text"/>	

Table 84: Static Addresses for Environments with Strict Firewall Policies


Section	Setting	Static URL/IP Address and Port
Update Servers (images):	Base URL (all services except Time zone rules and AsyncOS upgrades)	http://downloads-static.ironport.com 204.15.82.8 Port 80
	Base URL (Time zone rules)	downloads-static.ironport.com 204.15.82.8 Port 80
	Host (AsyncOS upgrades)	updates-static.ironport.com 208.90.58.25 Port 80

Section	Setting	Static URL/IP Address and Port
Update Servers (list):	For updates on physical hardware appliances: Full URL	update-manifests.ironport.com 208.90.58.5 Port 443
	For updates on virtual appliances: Full URL	update-manifests.sco.cisco.com Port 443
	For upgrades: Full URL	update-manifests.ironport.com 208.90.58.5 Port 443



Important You must configure the `update-manifests` URLs and port numbers using the `dynamichost` sub command of the `updateconfig` command in the CLI. This validates the service updates.

Configuring the Update and Upgrade Settings from the GUI

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Update Settings**.
- Step 3** Click **Edit Update Settings**.
- Use the descriptions in [Upgrade and Update Settings, on page 488](#) to configure the settings in this procedure.
- Step 4** In the **Update Servers (images)** section, specify the servers from which to download images for updates.
- Step 5** Specify the server from which to download images for AsyncOS upgrades:
- At the bottom of the same section, click the **Click to use different settings for AsyncOS upgrades** link.
 - Specify server settings for downloading images for AsyncOS upgrades.
- Step 6** In the **Update Servers (list)** section, specify the servers for obtaining the list of available updates and AsyncOS upgrades. The top subsection applies to updates. The bottom subsection applies to upgrades.
- Step 7** Specify settings for Time Zone rules and interface.
- Step 8** (Optional) Specify settings for Proxy Servers.
- Step 9** Submit and commit your changes.
- Step 10** Verify that your results are what you expect:
- If you are not already looking at the Update Settings page, choose **Management Appliance > System Administration > Update Settings**.
- Some URLs may append an “asynco” directory to the server URL. You can ignore this discrepancy.

Upgrade Notifications

By default, users with administrator and technician privileges will see a notification at the top of the web interface when an AsyncOS upgrade is available for the appliance.

To	Do This
View more information about the latest upgrade	Hover over the upgrade notification.
View a list of all available upgrades	Click the down arrow in the notification.
Dismiss a current notification. The appliance will not display another notification until a new upgrade becomes available.	Click the down arrow, then select Clear the notification , then click Close .
Prevent future notifications (Users with Administrator privileges only.)	Go to Management Appliance > System Administration > System Upgrade .

Before You Upgrade: Important Steps

Before you begin

See network requirements at [Determining Network Requirements for Upgrades and Updates](#), on page 485.

-
- Step 1** Take steps to prevent or minimize 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 [About Disk Space Maximums and Allocations](#), on page 522.
 - 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. See caveats at [Saving and Exporting the Current Configuration File](#), on page 514.
- If you need to revert to the pre-upgrade release for any reason, you will need this file.
- Step 3** If you are using the Safelist/Blocklist feature, export the list off the appliance.
- Click **Management Appliance > System Administration > Configuration File** and scroll down.
- 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.
- Step 6** Verify that the upgrade settings are configured as you want them. See [Configuring Upgrade and Service Update Settings](#), on page 487.
-

Upgrading AsyncOS


You can download and install in a single operation, or download in the background and install later.



Note When downloading and upgrading AsyncOS in a single operation from a local server instead of from a Cisco server, the upgrade installs immediately *while downloading*. A banner displays for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you have the option to type Control-C to exit the upgrade process before downloading starts.

Before you begin

- Choose whether you will download upgrades directly from Cisco or will host upgrade images from a server on your network. Then set up your network to support the method you choose. Then configure the appliance to obtain upgrades from your chosen source. See [Choosing an Upgrade Method: Remote vs. Streaming](#), on page 485 and [Configuring Upgrade and Service Update Settings](#), on page 487.
- Before installing the upgrade, follow the instructions in [Before You Upgrade: Important Steps](#), on page 492.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > System Upgrade**.

Step 3 Click **Upgrade Options**.

Step 4 Choose an option:

To	Do This
Download and install the upgrade in a single operation	Click Download and Install . If you have already downloaded an installer, you will be prompted to overwrite the existing download.
Download an upgrade installer	Click Download only . If you have already downloaded an installer, you will be prompted to overwrite the existing download. The installer downloads in the background without interrupting service.
Install a downloaded upgrade installer	Click Install . This option appears only if an installer has been downloaded. The AsyncOS version to be installed is noted below the Install option.

Step 5 Unless you are installing a previously-downloaded installer, select an AsyncOS version from the list of available upgrades.

Step 6 If you are installing:

- Choose whether or not to save the current configuration to the configuration directory on the appliance.
- Choose whether or not to mask the passphrases in the configuration file.

Note You cannot load a configuration file with masked passphrases using the Configuration File page in the GUI or the `loadconfig` command in the CLI.

- If you want to email copies of the configuration file, enter the email addresses to which you want to email the file. Use commas to separate multiple email addresses.

Step 7 Click **Proceed**.

Step 8 If you are installing:

- a) Be prepared to respond to prompts during the process.

The process pauses until you respond.

A progress bar appears near the top of the page.

- b) At the prompt, click **Reboot Now**.

Note Do not interrupt power to the appliance for any reason (even to troubleshoot an upgrade issue) until at least 20 minutes have passed since you rebooted.


- c) After about 10 minutes, access the appliance again and log in.

What to do next

- If the process was interrupted, you must start the process again.
- If you downloaded but did not install the upgrade:

When you are ready to install the upgrade, follow these instructions from the beginning, including the prerequisites in the Before You Begin section, but choose the Install option.
- If you installed the upgrade, see [After Upgrading](#), on page 495.

Viewing Status of, Canceling, or Deleting a Background Download

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > System Upgrade**.

Step 3 Click **Upgrade Options**.

Step 4 Choose an option:

To	Do This
View download status	Look in the middle of the page. If there is no download in progress and no completed download waiting to be installed, you will not see download status information. Upgrade status also appears in upgrade_logs.
Cancel a download	Click the Cancel Download button in the middle of the page. This option appears only while a download is in progress.
Delete a downloaded installer	Click the Delete File button in the middle of the page. This option appears only if an installer has been downloaded.

After Upgrading

After the upgrade is complete, complete the following:

- (For deployments with associated Email Security appliances) Re-enable the listeners.
- (For deployments with associated Web Security appliances) Configure your system to support the latest Configuration Master. See [Using Configuration Masters to Centrally Manage Web Security Appliances](#), on page 332.
- Consider saving your configuration. For more information, see [Saving and Importing Configuration Settings](#), on page 513.
- Before viewing the online help after upgrade, clear your browser cache, exit the browser, then open it again. This clears the browser cache of any outdated content.

About Reverting to an Earlier Version of AsyncOS

You can revert to an to a previous qualified version of AsyncOS for emergency uses.

You can also revert to the currently running build if you want to clear all data on the appliance and start with a new, clean configuration.

Related Topics

- [Important Note About Reversion Impact](#), on page 495
- [Reverting AsyncOS](#), on page 495

Important Note About Reversion Impact

Using the revert command on a Cisco Content Security appliance is a very destructive action. This command permanently destroys all existing configurations and data. In addition, it disrupts mail handling until the appliance is reconfigured.

Reverting does not affect feature key or virtual appliance license expiration dates.

Reverting AsyncOS

Before you begin

- Back up or save any data that you want to preserve to a location off the appliance.
- You must have a configuration file for the version you want to revert to. Configuration files are *not* backwards-compatible.
- Because this command destroys all configuration, it is highly recommended that you have physical local access to the appliance when reverting.
- If quarantines are enabled on your Email Security appliances, disable centralization so that messages are quarantined locally on those appliances.

- 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 passphrases 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:

Example:

```
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 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 passphrases
unmasked)
- exported the Cisco 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** Add at least one Web Security appliance and wait a few minutes to allow any URL Category updates to be downloaded from that appliance.
- Step 11** After URL Category updates are completed, load the XML configuration file of the version you are reverting to.
- Step 12** If you use the Safelist/Blocklist feature, import and restore the Safelist/Blocklist database.
- Step 13** Reenable any listeners on your Email Security appliances.
- Step 14** Commit your changes.

The reverted Cisco Content Security 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 Content Security appliance is available again.

About Updates

Service updates are periodically made available for download. To specify settings for these downloads, see [Configuring Upgrade and Service Update Settings, on page 487](#)

Related Topics

- [Configuring Upgrade and Service Update Settings, on page 487](#)

About URL Category Set Updates for Web Usage Controls

- [Preparing For and Managing URL Category Set Updates , on page 358](#)
- [URL Category Set Updates and Reports , on page 177](#)

Configuring the Appliance to Trust Proxy Server Communication

If you are using a non-transparent proxy server, you can add the CA certificate used to sign the proxy certificate to the email gateway. By doing so, the email gateway trusts the proxy server communication.

When Cisco Secure Email and Web Manager communicates with the updater servers to receive updates, a validation if the certificate is trusted is performed on the certificates that are used. To successfully validate the certificates used, you must include that updater server's Certificate Authority certificate into our Cisco Secure Email and Web Manager for successful communication. To perform this, use the **updateconfig > trusted_certificates** . The options in the command include:

- Add- To add a certificate in CA
- List- To list all the certificates in CA
- Delete- To delete a certificate in CA

Use the updateconfig command to configure this option. The following example shows how to configure this option.

```
SMA> updateconfig
```

```
Service (images): Update URL:
```

```
-----  
Feature Key updates http://downloads.ironport.com/asyncos
```

Configuring the Appliance to Trust Proxy Server Communication

```

Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:
-----
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

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

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

Paste certificates to be trusted for secure updaters connections, blank to quit
Trusted Certificate for Updater:
paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIIOUMAFHhzRskwDQYJKoZIhvcNAQELBQAwczELMAkGA1UE
BhMCSU4xCzAJBgNVBAGTA1ROMQwwCgYDVQQHEwNDaG4xETAPBgNVBAoTCENBQ053
aWxkMREwDwYDVQQLEwhDQUNOd2lsZDEjMCEGA1UEAwwaKi5jczIxLmRldml0LmNp
c2NvbGFiY3Y5b20wHhcNMjE1MTE0NzAwWhcNMjE1MTE0NzAwWjBzMQswCQYDVQ
QGEwJTTjELMAkGA1UECBMVE4xZDAKBgNVBAcTA0NobjERMA8GA1UEChMIQ0FDND
pbgGQxETAPBgNVBAsTCENBQ053aWxkMStMwIQYDVQQDDBoqLmNzZmJmZjEuZGV2
aXQuY2lyZ29sYWJzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJPPBRGq0wHv/6ZLPOZ3jdEgzVS+dzXJSyhtMsgm/XrvIvjRH0MK3r++dtUgHMz
le/WrxPKGphjtNsvF7ss58RRg3fiQCSQPX6nfBYc9v4A7rSdmKzYYFbBkGPeijLB
qwVyseMa3rifjv4Bucxw0M3ZrUqq7YfcZtxZhSetxx8rt3A/uReIm/n1ERcZDclW
+GkfrXEdY3ZLpen/2sFiOAVMvAHlKRtK7kEhmo1TPQZ0h0UQFNDb12ZWZZ6Nuv0I
Z6pUDNj1/+GoJyvSwl0qpetHxhdMtubMAAM8JQNvNkHgZOsWSbN18F5at7cz/KFI
HuvBUXKHV5pEX3hOdJxbuocCAwEAAANdMFswDAYDVR0TBAAUwAwEB/zAdBgNVHQ4E
FgQUCN1XseZ5qBjJtYv3sdCujJuqnAwHwYDVR0jBBGwFoAUCN1XseZ5qBjJtYv
3sdCujJuqnAwCwYDVR0PBAQDAGGMA0GCSqGSIb3DQEBCwUAA4IBAQBaq5KXw/wX
nzJpBnKPZu04KNCIz9/A2Hil2ikWNBjfla1x/37OdTbh3IpHJ6n1OCeAke5Ww7uX
amlUcWxvDk3Zn+tKysCU2Q1PYSxUHXtqH3rvWZDRglPkJUu420tnCg2fV1bulcJ1
xx6E95a9D1vCarfxvUINU50076gnyptMv9+1OFXCkvDgBomkQpqsWR51519kmDzi
mt8CoknJN/iAENxM8b47262yXec1X6ZN/Owa/x14OS3X0C0hiky9HpUGDq+CigE
s5CBCOLDfe8G9kAPoTg2mVNT10xxQF1juobb6djmdB1Of8kqgKs2eWsd+MfKvNbG
ZzPGx4SUS2RZ
-----END CERTIFICATE-----
.
Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain
Name (FQDN) format ? [N]> y

```



```

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

```

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.

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

The appliance sends you email alerts about events occurring on the appliance.

To	Do This
Have different types of alerts sent to different administrative users	<p>Select Management Appliance > System Administration > Alerts</p> <p>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.</p> <p>Separate multiple addresses with commas.</p>
Configure global settings for alerts, including: <ul style="list-style-type: none"> • Alert sender (FROM:) address • Controls for duplicate alerts • AutoSupport settings. 	<p>Select Management Appliance > System Administration > Alerts</p> <p>See About Duplicate Alerts , on page 501</p> <p>See Cisco AutoSupport, on page 501</p>
View a list of recent alerts Manage settings for this list	<p>See Viewing Recent Alerts , on page 501</p>
See a list of alerts and their descriptions	<p>See:</p> <p>Hardware Alert Descriptions , on page 502.</p> <p>System Alert Descriptions , on page 502</p>
Understand alert delivery mechanisms	<p>See Alert Delivery, on page 500</p>

Alert Types and Severities

Alert types include:

- Hardware alerts. See [Hardware Alert Descriptions](#) , on page 502.
- System alerts. See [System Alert Descriptions](#) , on page 502.
- Updater alerts.

Alerts can have 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 Delivery

Because alert messages can be used to inform you of problems within your Cisco Content Security 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 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.
- If your deployment includes Email Security appliances:
 - 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.
- [Optional - Only if TLS support is enabled in "alertconfig" and FQDN validation enabled in SSL Configuration settings]: Check whether the 'Common Name,' 'SAN: DNS Name' fields, or both present in the server certificate, are in the FQDN format.
- [Optional - Only if TLS support is enabled in "alertconfig"]: Check whether the 'Common Name,' or 'SAN: DNS Name' fields, of the server certificate contain Hostname of the server. Reverse DNS name is used if IP is configured in Hostname field.
- [Optional - Only if TLS support is enabled using the `alertconfig` CLI command]: Check whether the server name is present in the 'Common Name' or 'SAN: DNS Name' fields in the server certificate.
- [Optional - Only if TLS support is enabled using the `alertconfig` CLI command and X 509 validation is enabled on the SSL Configuration page]: Check the server certificate version.

Viewing Recent Alerts

To	Do This
View a list of recent alerts	Users with administrator and operator access can choose Management Appliance > System Administration > Alerts and click the View Top Alerts button. Alerts appear even if there was a problem emailing them.
Sort the list	Click a column heading.
Specify the maximum number of alerts to save in this list	Use the alertconfig command in the command-line interface
Disable this feature	Use the alertconfig command in the command-line interface to set the maximum number of alerts to zero (0).

About 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.

Cisco AutoSupport

To allow Cisco to better support and design future system changes, the Cisco Content Security appliance can be configured to send Cisco a copy of all alert messages generated by the system. This feature, called 'AutoSupport', is a useful way to allow 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. This can be disabled if you do not want to send the weekly alert messages internally. To enable or disable this feature, select **Management Appliance > System Administration Alerts** and click edit settings.

By default, if AutoSupport is enabled, the weekly AutoSupport report is sent to alert recipients set to receive system alerts at the Information level.

Hardware Alert Descriptions

Table 85: Hardware Alert Descriptions

Alert Name	Description	Severity
INTERFACE.ERRORS	Sent when interface errors are detected.	Warning
MAIL.MEASUREMENTS_FILESYSTEM	Sent when a disk partition is nearing capacity (75%).	Warning
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	Sent when a disk partition reaches 90% capacity (and at 95%, 96%, 97%, and so on).	Critical
SYSTEM.RAID_EVENT_ALERT	Sent when a critical RAID-event occurs.	Warning
SYSTEM.RAID_EVENT_ALERT_INFO	Sent when a RAID-event occurs.	Information

System Alert Descriptions

Table 86: System Alert Descriptions

Alert Name	Description	Severity
COMMON.APP_FAILURE	Sent when there is an unknown application failure.	Critical
COMMON.KEY_EXPIRED_ALERT	Sent when a feature key has expired.	Warning
COMMON.KEY_EXPIRING_ALERT	Sent when a feature key is about to expire.	Warning
COMMON.KEY_FINAL_EXPIRING_ALERT	Sent as a final notice that a feature key is about to expire.	Warning
DNS.BOOTSTRAP_FAILED	Sent when the appliance is unable to contact the root DNS servers.	Warning
COMMON.INVALID_FILTER	Sent when an invalid filter is encountered.	Warning

Alert Name	Description	Severity
IPBLOCKD.HOST_ADDED_TO_ALLOWED LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED LIST	<p>Alert messages:</p> <ul style="list-style-type: none"> • The host at <IP address> has been added to the blocked list because of an SSH DOS attack. • The host at <IP address> has been permanently added to the ssh allowed list. • The host at <IP address> has been removed from the blocked list. <p>IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blocked list if more than 10 failed attempts occur within two minutes.</p> <p>When a user logs in successfully from the same IP address, that IP address is added to the allowed list.</p> <p>Addresses on the allowed list are allowed access even if they are also on the blocked list.</p>	Warning
LDAP.GROUP_QUERY_FAILED_ALERT	Sent when an LDAP group query fails.	Critical
LDAP.HARD_ERROR	Sent when an LDAP query fails completely (after trying all servers).	Critical
LOG.ERROR.*	Various logging errors.	Critical
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	Sent when an LDAP group query fails during per-recipient scanning.	Critical
MAIL.QUEUE.ERROR.*	Various mail queue hard errors.	Critical
MAIL.RES_CON_START_ALERT.MEMORY	Sent when RAM utilization has exceeded the system resource conservation threshold.	Critical
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	Sent when the mail queue is overloaded and system resource conservation is enabled.	Critical

Alert Name	Description	Severity
MAIL.RES_CON_START_ALERT.QUEUE	Sent when queue utilization has exceeded the system resource conservation threshold.	Critical
MAIL.RES_CON_START_ALERT.WORKQ	Sent when listeners are suspended because the work queue size is too big.	Critical
MAIL.RES_CON_START_ALERT	Sent when the appliance enters “resource conservation” mode.	Critical
MAIL.RES_CON_STOP_ALERT	Sent when the appliance leaves “resource conservation” mode.	Critical
MAIL.WORK_QUEUE_PAUSED_NATURAL	Sent when the work queue is paused.	Critical
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	Sent when the work queue is resumed.	Critical
NTP.NOT_ROOT	Sent when the appliance is unable to adjust time because NTP is not running as root.	Warning
PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS	Sent when errors are found in the domain specification file.	Critical
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY	Sent when the domain specification file is empty.	Critical
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING	Sent when the domain specification file is not found.	Critical
REPORTD.DATABASE_OPEN_FAILED_ALERT	Sent if the reporting engine is unable to open the database.	Critical
REPORTD.AGGREGATION_DISABLED_ALERT	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
REPORTD.DATABASE_DELETION_ALERT	Sent if system checks and finds the export directory is not empty, then it prints the logline and tries to delete the directory in the next iteration.	Information
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Sent if the reporting engine was unable to save reporting data.	Warning

Alert Name	Description	Severity
REPORTING.CLIENT.JOURNAL.FULL	Sent if the reporting engine is unable to store new data.	Critical
REPORTING.CLIENT.JOURNAL.FREE	Sent when the reporting engine is again able to store new data.	Information
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE_ALERT	Sent when the reporting engine is unable to build a report.	Critical
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE_ALERT	Sent when a report could not be emailed.	Critical
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE_ALERT	Sent when a report could not be archived.	Critical
SENDERBASE.ERROR	Sent when an error occurred while processing a response from SenderBase.	Information
SMAD.ICCM.ALERT_PUSH_FAILED	Sent if a configuration push failed for one or more hosts.	Warning
SMAD.TRANSFER.TRANSFERS_STALLED	Sent if SMA logs are unable to fetch tracking data for two hours or reporting data for six hours.	Warning
SMTPAUTH.FWD_SERVER_FAILED_ALERT	Sent when the SMTP Authentication forwarding server is unreachable.	Warning
SMTPAUTH.LDAP_QUERY_FAILED	Sent when an LDAP query fails.	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT	Sent when there was a problem shutting down the system on reboot.	Warning
SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN	Sent when there was a problem shutting down the system.	Warning
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Sent when a recipient validation update failed.	Critical
SYSTEM.SERVICE_TUNNEL.DISABLED	Sent when a tunnel created for Cisco Support Services is disabled.	Information
SYSTEM.SERVICE_TUNNEL.ENABLED	Sent when a tunnel created for Cisco Support Services is enabled.	Information

Changing Network Settings

This section describes the features used to configure the network operation of the appliance. These features give you direct access to the hostname, DNS, and routing settings that you configured using the System Setup Wizard in [Running the System Setup Wizard, on page 15](#).

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`
- Passphrase

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 content security 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 content security 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 87: 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 Content Security 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, on page 507](#).

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 IronPort AsyncOS CLI Reference Guide, available from the location specified in [Documentation , on page 629](#)), 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

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Network > DNS** page and click the **Edit Settings** button.
- Step 3** Select whether to use the Internet’s root DNS servers or your own internal DNS server(s), and specify authoritative DNS servers.
- Step 4** 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, on page 507](#).
- Step 5** Choose an interface for DNS traffic.
- Step 6** Enter the number of seconds to wait before canceling a reverse DNS lookup.
- Step 7** Optionally, clear the DNS cache by clicking **Clear Cache**.

Step 8 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, on page 509](#)
- [Modifying the Default Gateway \(GUI\), on page 509](#)

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.



Note If the destination is a subnet and not a single IP address, ensure that the entry adheres to CIDR (Classless Inter-Domain Routing) notation, for example, 192.168.90.0/24.

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** On the **Management Appliance > Network > Routing** page, click **Add Route** in the route listing. The 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.
-

Modifying the Default Gateway (GUI)

- Step 1** Click Default Route in the route listing on the Routing page.
- 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 \(GUI\), on page 509](#)) or via the `setgateway` command in the CLI.

Secure Communication Protocol

If you plan to upgrade from a lower AsyncOS version (for example, 13.6.x) with TLSv1.0 enabled to AsyncOS 13.8.x and later, then TLSv1.0 is disabled, TLSv1.1 and TLSv1.2 are enabled by default. You need to enable the TLSv1.0 method on your appliance after the upgrade.

From AsyncOS 15.5 and later, it is recommended to use TLSv1.1, TLSv1.2, and TLSv1.3 (for Appliance Management Web User Interface) methods instead of TLSv1.0. TLSv1.3 is disabled by default, and you must enable it.

Specifying a Secure Communication Protocol

You can choose the communication protocol to be used for each of the following services:

- Appliance Management Web User Interface
- Secure LDAP Services
- Updater Service
- End-User Access to the Spam Quarantine



Note The Updater Service and Secure LDAP Services use TLSv1.1 and TLSv1.2 methods on a newly installed appliance. The Appliance Management Web User Interface uses TLSv1.1 and TLSv1.2 methods by default, and TLSv1.3 method is disabled by default on a newly installed appliance.

To view the currently selected protocols and available options or to change protocols, use the `sslconfig` command in the command-line interface. The changes made using the `sslconfig` command require a Commit. The affected services will be briefly interrupted after you commit changes using the `sslconfig` command.

If you are using a local (remote) Updater Service and for all other services and web browsers, the protocol you choose must be supported by and enabled on the server and tools you use. One of the available options must be enabled for each service you use.

For information on Peer Certificate FQDN Validation, see [FQDN, on page 554](#).

For information on Peer Certificate X509 Validation, see [X.509 Certificate, on page 556](#).

Configuring the System Time



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, see [How the Security Management Appliance Gathers Data for Reports, on page 24](#).

To set time-related settings using the command-line interface, use the `ntpconfig`, `settime`, and `settz` commands.

To	Do This
Set the system time	<p>Select Management Appliance > System Administration > Time Settings</p> <p>See also Using a Network Time Protocol (NTP) Server, on page 511</p>
Set the time zone	<p>Select Management Appliance > System Administration > Time Zone</p> <p>See also:</p> <ul style="list-style-type: none"> • Selecting a GMT Offset, on page 512 • Updating Time Zone Files, on page 512

Using a Network Time Protocol (NTP) Server

You can use a Network Time Protocol (NTP) server to synchronize the Security Management appliance system clock with other computers on your network or the internet.

The default NTP server is `time.sco.cisco.com`.

If you will use an external NTP server, including the default NTP server, open the required port through the firewall. See [Firewall Information, on page 621](#)

Related Topics

- [Configuring the System Time, on page 510](#)
- [Manually Updating Time Zone Files , on page 512](#)


(Recommended) Setting Appliance System Time Using the Network Time Protocol (NTP)

This is the recommended time keeping method, especially if your appliance is integrated with other devices. All integrated devices should use the same NTP server.

You can use the `ntpconfig` command in the CLI to setup the time using the NTP server.

-
- Step 1** Go to the **System Administration > Time Settings** page.
- Step 2** Click **Edit Settings**.
- Step 3** In the Time Keeping Method section, select **Use Network Time Protocol**.
- Step 4** Enter an NTP server address and click **Add Row**. You can add multiple NTP servers .
- Step 5** To delete an NTP server from the list, click the trash can icon for that server.
- Step 6** Select an interface for NTP queries. This is the IP address from which NTP queries should originate.
- Step 7** Select the **Use NTP Authentication** check box to ensure that a timestamp is generated by a trusted source, protecting NTP from malicious activity or interception.
- Step 8** Submit and commit your changes.
-

Selecting a GMT Offset


- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Time Zone**.
- Step 3** Click **Edit Settings**.
- Step 4** Select GMT Offset from the list of regions. The Time Zone Setting page is updated to include GMT offsets in the Time Zone field.
- Step 5** 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 6** Submit and commit your changes.
-

Updating Time Zone Files


Whenever there is a change in the time zone rules for any country, Time Zone files on the appliance must be updated.

- [Automatically Updating Time Zone Files](#) , on page 512
- [Manually Updating Time Zone Files](#) , on page 512

Automatically Updating Time Zone Files

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Update Settings**.
- Step 3** Select the **Enable automatic updates for Time zone rules** check box.
- Step 4** Enter an interval. Click the ? help on the page for important information.
- Step 5** Submit and commit your changes.
-

Manually Updating Time Zone Files

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Time Settings**.
- Step 3** Look at the **Time Zone File Updates** section.
- Step 4** If there is an available time zone file update, click **Update Now**.
-

Configuration File Page

For Information About This Section	See
Saving the current configuration	Saving and Importing Configuration Settings , on page 513
Loading a saved configuration	Saving and Importing Configuration Settings , on page 513
End-User Safelist/Blocklist Database (Spam Quarantine)	Backing Up and Restoring the Safelist/Blocklist , on page 285
Reset Configuration	Resetting the Configuration to Factory Defaults , on page 470

Saving and Importing Configuration Settings



Note The configuration file described in this section is used to configure Security Management appliances.

Most configuration settings for the Security Management 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:

- In case of unexpected disaster to your primary Security Management appliance, you can quickly configure a second Security Management appliance to restore service.
- 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.)
- You can use the configuration file to speed configuration of another appliance, for example a cloned virtual appliance.

Managing Configuration Files

- [Backing Up and Restoring the Safelist/Blocklist](#) , on page 285

- [Resetting the Configuration to Factory Defaults, on page 470](#)
- [Rolling Back to a Previously Committed Configuration , on page 516](#)

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.

Masking the passphrase

Optionally, mask the user's passphrases by selecting the check box. Masking a passphrase causes the original, encrypted passphrase to be replaced with "*****" in the exported or saved file.



Note Configuration files with masked passphrases cannot be loaded back into AsyncOS.

Encrypting the passphrase

You can encrypt the user's passphrases by clicking the Encrypt passphrases in the Configuration Files checkbox. The following are the critical security parameters in the configuration file that will be encrypted.

- Certificate private keys
- RADIUS passwords
- LDAP bind passwords
- Local users' password hashes
- SNMP password
- Outgoing SMTP authentication passwords
- PostX encryption keys
- PostX encryption proxy password
- FTP Push log subscriptions' passwords
- IPMI LAN password
- Updater server URLs

You can also configure this in the command-line interface using the `saveconfig` command.

Loading a Configuration File

The configuration file must have been saved from an appliance running the same AsyncOS version as the appliance on which you will load the configuration.

Configuration files with masked passphrases cannot be loaded.

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 Content Security 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 any import 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.



Caution 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>
```



Caution 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 Passphrases for Log Subscriptions

If you attempt to load a configuration file that contains a log subscription that requires a passphrase (for example, one that will use FTP push), the `loadconfig` command does not warn you about the missing passphrase. The FTP push fails and alerts are generated until you configure the correct passphrase 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"?>
```

Resetting the Current Configuration

Resetting the current configuration causes your Cisco Content Security appliance to revert settings back to the original factory defaults. Save your configuration prior to resetting it.

See [Resetting the Configuration to Factory Defaults, on page 470](#).

Rolling Back to a Previously Committed Configuration

You can roll back the configuration to a previously-committed configuration.

Use the `rollbackconfig` command in the command-line interface to choose one of the ten most recent commits.

If you enter No when prompted to commit a rollback, the rollback will be committed the next time you commit changes.

Only users with Administrator access can use the `rollbackconfig` command.



Note No log messages or alerts will be generated when a previous configuration is restored.



Note Certain commits, such as re-allocating disk space to a size insufficient to hold existing data, could result in data loss.

CLI Commands for Configuration Files

The following commands enable you to manipulate the configuration files:

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `rollbackconfig`
- `resetconfig` (see [Resetting the Configuration to Factory Defaults, on page 470](#))
- `publishconfig`
- `backupconfig` (see [Backing Up Security Management Appliance Data , on page 476](#))
- `trailblazerconfig`

The `showconfig`, `mailconfig`, and `saveconfig` Commands

For the configuration commands `showconfig`, `mailconfig`, and `saveconfig`, you are prompted to choose whether to include passphrases in the file that will be mailed or displayed. Choosing not to include passphrases leaves any passphrase field blank. You can choose not to include passphrases if you are concerned about security breaches. However, configuration files without passphrases fail when loaded using the `loadconfig` command. See [Note About Loading Passphrases for Log Subscriptions, on page 516](#).



Note When saving, showing, or mailing your configuration file if you choose to include passphrases (answer yes to “Do you want to include passphrases?”), the passphrases 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 passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: 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 passphrases? Please be aware that a configuration
without passphrases 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) with a unique filename to the configuration directory.

```
mail3.example.com> saveconfig
Do you want to include passphrases? Please be aware that a configuration without passphrases
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 appliance. You can load information using one of two methods:

- Placing information in the configuration directory and uploading it
- Pasting configuration information directly into the CLI

See [Loading a Configuration File, on page 514](#) for more information.

The rollbackconfig Command

See [Rolling Back to a Previously Committed Configuration , on page 516](#).

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 the Compatibility Matrix in the Release Notes for this release at http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html . 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 trailblazerconfig Command

You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.

You can see the inline help by using the following command on the CLI: `help trailblazerconfig`.

The syntax is as follows:

```
trailblazerconfig enable <https_port> <http_port>
trailblazerconfig disable
trailblazerconfig status
```

Where:

'enable' runs the trailblazer configuration on the default ports (HTTPS: 4431).

'disable' disables the trailblazer configuration

'status' checks the status of the trailblazer configuration.



Important By default, `trailblazerconfig` CLI command is enabled on your appliance. Make sure that the HTTPS ports are opened on the firewall. Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

The `trailblazerconfig` command helps you to avoid the following issues:

- Requiring to add multiple certificates for API ports in certain browsers.
- Redirecting to the legacy web interface when you refresh the Spam quarantine, Safelist or Blocklist page.
- Metrics bar on the Advanced Malware Protection report page does not contain any data.



Note When you enable `trailblazerconfig` command on the appliance, the request URL will contain the `trailblazerconfig` HTTPS port number appended to the hostname.

The updatevocert Command

You must use the `updatevocert` command in the CLI to update the CA certificate of 2048 bits to enable Centralized Policy, Virus and Quarantines on the managed Cisco Email Security appliance that is in FIPS mode.

The Centralized Policy, Virus, and Outbreak Quarantines on the managed Email Security appliance is disabled when FIPS is enabled. From AsyncOS 13.0 onwards, appliances in FIPS mode uses a certificate of 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines. The earlier AsyncOS versions have certificates of size 1024 bits.

```
example.mail.com> updatevocert
This command will recreate the PVO certificate and key of strength 2048 bits.
Also, the new certificate will be signed by a CA of strength 2048 bits.
Hermes process will restart post certificate update. No commit will be required.
Do you want to proceed with the certificate update? [Y]>

Certificate updated successfully. Hermes restart needed for the changes to be effective.
Do you want to restart hermes? [Y]> Y

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

Waiting for listeners to exit... Receiving suspended for euq_listener, cpq_listener. Waiting
```

```

    for outgoing deliveries to finish... Mail delivery suspended. Receiving resumed for
    euq_listener, cpq_listener. Mail delivery resumed.
    Hermes will be up in a moment. Run the status command for hermes.

example.mail.com >

```

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 [IP Interfaces and Accessing the Appliance, on page 609](#) 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:

Example:

```

mail3.example.com>
1
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 [Running the System Setup Wizard, on page 15](#).) Finally, the changes are committed.

Example:

```

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 Space

You can allocate available disk space among the features that your organization uses, up to the maximum available.

- [\(Virtual Appliances Only\) Increasing Available Disk Space](#) , on page 521
- [Viewing Disk Space, Quotas and Usage](#) , on page 522
- [About Disk Space Maximums and Allocations](#), on page 522
- [Ensuring That You Receive Alerts About Disk Space](#) , on page 522
- [Managing Disk Space for the Miscellaneous Quota](#) , on page 523
- [Reallocating Disk Space Quotas](#) , on page 523

(Virtual Appliances Only) Increasing Available Disk Space

For virtual appliances running ESXi 5.5 and VMFS 5, you can allocate more than 2TB of disk space. For appliances running ESXi 5.1, the limit is 2 TB.



Note Disk space reduction in ESXi is not supported. See the VMWare documentation for information.

To add disk space to the virtual appliance instance:

Before you begin


Carefully determine the disk space increase needed.

Step 1 Bring down the Cisco Content Security Management appliance instance.

Step 2 Increase disk space using utilities or administrative tools provided by VMWare.

See information about changing the virtual disk configuration in the VMWare documentation.

Information for ESXi 5.5 is available here: <http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html>

Step 3 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 4 Go to **Management Appliance > System Administration > Disk Management** and verify that your change has taken effect.

Viewing Disk Space, Quotas and Usage

To	Do This
View the total disk space available on the appliance	Select Management Appliance > System Administration > Disk Management . Look at the values shown for "Total Space Allocated" - for example, 184G of 204G.
View the amount of disk space allocated to and currently used by each of the Security Management appliance's monitoring services	Select Management Appliance > System Administration > Disk Management .
View the percentage of the quotas for quarantines that are currently used	Select Management Appliance > Centralized Services > System Status and look at the Centralized Services section.

About Disk Space Maximums and Allocations



Note Centralized Reporting Disk Space on Security Management appliances is used for both Email and Web data. If you enable either Centralized Email Reporting or Centralized Web Reporting, all of the space is dedicated to the enabled feature. If you enable both, Email and Web reporting data share the space and space is allocated on a first-come basis.

- If you enable centralized web reporting but there is no disk space allocated for reporting, then centralized web reporting will not work until disk space is allocated.
- Before reducing the Miscellaneous quota below current usage levels, you should delete unneeded data. See [Managing Disk Space for the Miscellaneous Quota](#) , on page 523.
- For more information about how disk space is managed for policy, virus, and outbreak quarantines, see [Disk Space Allocation for Policy, Virus, and Outbreak Quarantines](#) , on page 312 and [Retention Time for Messages in Quarantines](#) , on page 312.
- For all other data types, if you reduce the existing allocation below current usage, then the oldest data is deleted until all data fits within the new allocation amount.
- If the new quota is larger than the currently used disk space, you will not lose data.
- If you set the allocation to zero, no data is retained.

Ensuring That You Receive Alerts About Disk Space

You will begin to receive system alerts at warning level when Miscellaneous disk usage reaches 75% of the quota. You should take action when you receive these alerts.

To ensure that you receive these alerts, see [Managing Alerts](#), on page 499.

Managing Disk Space for the Miscellaneous Quota

The Miscellaneous quota includes System data and User data. You cannot delete System data. User data that you can manage includes the following types of files:

To Manage	Do this
Log files	Go to Management Appliance > System Administration > Log Subscriptions and: <ul style="list-style-type: none"> • Click the Size column heading to see which logs consume the most disk space. • Verify that you need all of the log subscriptions that are being generated. • Verify that the log level is no more verbose than necessary. • If feasible, reduce the rollover file size.
Packet captures	Go to Help and Support (near the upper right side of your screen) > Packet Capture . Delete any unneeded captures.
Configuration files (These files are unlikely to consume much disk space.)	FTP to the /data/pub directory on the appliance. To configure FTP access to the appliance, see Accessing the Appliance via FTP, on page 611
Quota size	Go to System Administration > Disk Management .


Reallocating Disk Space Quotas

If disk space is allocated to features you do not use, or if the appliance frequently runs out of disk space for a particular feature and has excess space for other features, you can reallocate disk space.

If you require more space for all features, consider upgrading your hardware or allocating more disk space to your virtual appliance. See [\(Virtual Appliances Only\) Increasing Available Disk Space, on page 521](#).

Before you begin

- Changing disk allocations may impact existing data or feature availability. See information at [About Disk Space Maximums and Allocations, on page 522](#).
- You can temporarily create space in a quarantine by manually releasing or deleting messages from the quarantine.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > Disk Management**
- Step 3** Click **Edit Disk Quotas**.
- Step 4** On the **Edit Disk Quotas** page, enter the amount of disk space (in gigabytes) allocated to each service.
- Step 5** Click **Submit**.
- Step 6** Click **Commit** to commit your changes.
-

Managing Data Storage Time

You can now configure your Secure Email and Web Manager to store the messages (data) in the Centralized Email Tracking database based on the number of days.

Use the **Apply Data Storage Time** option in System Administration > Disk Management > Edit Data Disk Management page of the legacy web interface to configure the data storage time.

The 'Apply Data Storage Time' option is applicable in any one of the following scenarios:

- If the configured data disk storage limit is reached (for example 500 GB), the messages are automatically deleted from the database even before the configured data storage time is reached (for example, '40 days').
- If the configured data storage time limit is 40 days and a message that is older than the configured data storage time limit (for example, '41 days'), the message is automatically deleted even if the configured data disk storage limit is not reached (for example '500 GB').



Note You can also use the 'Manage data based on the storage time' statement in the `diskquotaconfig > edit > Centralized Email Tracking` sub command in the CLI to store messages in the Centralized Email Tracking database based on the number of days.

Important: From Secure Email and Web Manager 13.6.2 version, the Splunk database is no longer used for email tracking data. All new email tracking data is stored in the Lucene database. When you use the 'Apply Data Storage Time' option, the Splunk database that contains the email tracking data gets deleted automatically.


Action: Make sure you take a backup of the email tracking data (if required). You can use the `backupconfig` command in the CLI to perform the backup action. For more information, see [Scheduling Single or Recurring Backups, on page 479](#).



Note If your organization network has only one Secure Email and Web Manager, you need to deploy a new Virtual Machine (VM) in the network. For more information on how to deploy a virtual Secure Email and Web Manager, see [Cisco Secure Email and Web Virtual Appliance Installation Guide](#).

Before you begin

Make sure you have a valid feature key for the Centralized Email Tracking service.


-
- Step 1** [New Web Interface Only] Click  on Secure Email and Web Manager to load the legacy web interface.
 - Step 2** Choose **Management Appliance > System Administration > Disk Management**.
 - Step 3** Click **Edit Disk Quotas**.
 - Step 4** Select **Apply Data Storage Time** under Centralized Email Tracking and enter a value in the given field to store the messages (data) in the Centralized Email Tracking database based on the number of days.
 - Step 5** Click **Submit**.

Step 6 Click **Commit** to commit your changes.

Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances



Note To receive alerts related to these thresholds, configure the thresholds on each managed Email Security appliance. For information, see information about configuring thresholds for system health in the user guide or online help for your Email Security appliance release. You can also run on-demand system health checks from individual appliances. See information about checking the health of your appliance in the user guide or online help for your Email Security appliance release.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Click **Management Appliance > System Administration > System Health**.

Step 3 Click **Edit Settings**.

Step 4 Configure options.

Option	Description
Overall CPU Usage	Default: 85%
Memory Page Swapping	Default: 5000 pages
Maximum Messages in Work Queue	Default: 500 messages

Step 5 Submit and commit your changes.

SSO Using SAML 2.0

- [About SSO and SAML 2.0, on page 525](#)
- [SAML 2.0 SSO Workflow, on page 526](#)
- [Guidelines and Limitations for SAML 2.0, on page 527](#)
- [How to Configure SSO for Spam Quarantine, on page 534](#)
- [How to Configure SSO on your Cisco Security Management Appliance, on page 527](#)

About SSO and SAML 2.0

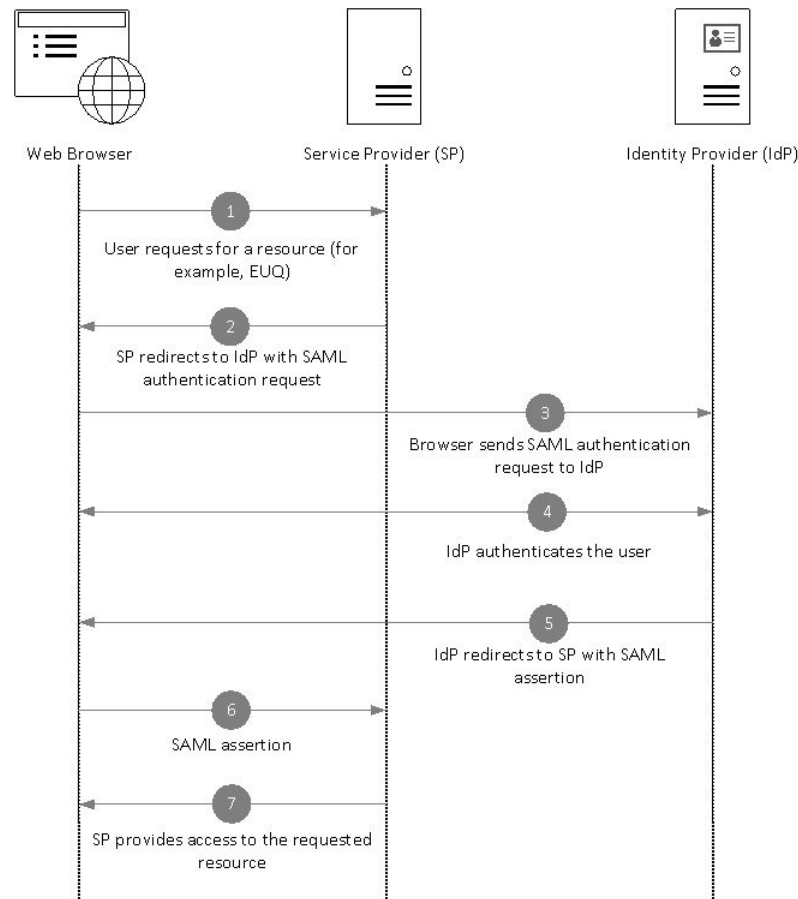
Cisco Content Security Management appliance now supports SAML 2.0 SSO so that the end users can access the Spam Quarantine using the same credentials that are used to access other SAML 2.0 SSO enabled services

within their organization. For instance, you have enabled Ping Identity as your SAML identity provider (IdP) and has accounts on Rally, Salesforce, and Dropbox which have been SAML 2.0 SSO enabled. When you configure Cisco Content Security Management appliance to support SAML 2.0 SSO as a Service Provider (SP), end users will be able to sign in once and have access to all these services including Spam Quarantine.

SAML 2.0 SSO Workflow

The SAML 2.0 SSO workflow is displayed in the following figure:

Figure 20: SAML 2.0 SSO Workflow



Workflow

1. The end user uses a web browser to request a resource from the service provider (your appliance). For example, the end user clicks on the spam quarantine link in a spam notification.
2. The service provider redirects the request to the web browser with SAML authentication request.
3. The web browser relays the SAML authentication request to the identity provider.
4. The identity provider authenticates the end user. The identity provider displays a login page to the end user and the end user logs in.
5. The identity provider generates the SAML assertion and sends it back to the web browser.

6. The web browser relays the SAML assertion to the service provider.
7. The service provider grants access to the requested resource.

Guidelines and Limitations for SAML 2.0

- [Logout, on page 527](#)
- [General, on page 527](#)
- [Spam Quarantine Access for Administrators, on page 527](#)

Logout

When end users log out of Spam Quarantine, they are not logged out of other SAML 2.0 SSO enabled applications.

General

You can configure only one instance of service provider and identity provider on Cisco Content Security Management appliance.

Spam Quarantine Access for Administrators

If you are enabling SSO for Spam Quarantine, keep in mind that the administrators will no longer be able to access the Spam Quarantine using the Spam Quarantine URL (http://<appliance_hostname>:<port>). Administrators can access the Spam Quarantine using the web interface (**Email > Message Quarantine > Spam Quarantine**).

How to Configure SSO on your Cisco Security Management Appliance

Procedure

	Command or Action	Purpose
Step 1	Review the prerequisites.	Prerequisites, on page 527
Step 2	Configure your appliance as a service provider.	Configure Cisco Content Security Management Appliance as a Service Provider, on page 528
Step 3	[On IDP] Configure the identity provider to work with your appliance.	Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 530
Step 4	Configure identity provider settings on your appliance.	Configure Identity Provider Settings on Cisco Content Security Management Appliance, on page 532
Step 5	Enable external authentication using SAML on your appliance.	Enable SAML Authentication, on page 533

Prerequisites

- [Supported Identity Providers, on page 528](#)

- [Certificates for Secure Communication, on page 528](#)

Supported Identity Providers

Verify whether the identity provider used by your organization is supported by Cisco Email Security Appliance. The following are the supported identity providers:

- Microsoft Active Directory Federation Services (AD FS) 2.0 and later
- Duo Access Gateway
- Azure AD

Certificates for Secure Communication

Obtain the following certificates that are required to secure the communication between your appliance and the identity provider:

- If you want your appliance to sign SAML authentication requests or if you want your identity provider to encrypt SAML assertions, obtain a self-signed certificate or a certificate from a trusted CA and the associated private key.
- If you want the identity provider to sign SAML assertions, obtain the identity provider's certificate and import the same to your appliance. Your appliance will use this certificate to verify the signed SAML assertions.

Converting Certificates

Normally, the certificates obtained from the appliance are in .pfx format and must be converted to .pem format when you configure your appliance as a service provider.


To convert the certificates from .pfx format to .pem format, do the following:

- Download and install OpenSSL tool and import the certificate file (.pfx) obtained from your appliance.
- Run the following command to export the certificate in .pem format: `openssl pkcs12 -in <certname>.pfx -nokeys -out cert.pem`
- Run the following command to export the private key in .pem format: `openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
- Run the following command to remove the passphrase from the private key: `openssl rsa -in key.pem -out server.key`

Configure Cisco Content Security Management Appliance as a Service Provider

Before you begin

Review the [Prerequisites, on page 527](#).

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > SAML**.
- Step 3** Under the Service Provider section, click **Add Service Provider**.

Step 4 Enter the following details:

Field	Description
Profile Name	Enter a name for the service provider profile.
Configuration Settings	
Entity ID	Enter a globally unique name for the service provider (in this case, your appliance). The format of the service provider Entity ID is typically a URI.
Name ID Format	The format that the identity provider should use to specify the user in the SAML assertion. This field is not configurable. You will need this value while configuring the identity provider.
Assertion Consumer URL	The URL to which the identity provider should send the SAML assertion after authentication has successfully completed. In this case, this is the URL to your spam quarantine. This field is not configurable. You will need this value while configuring the identity provider.
SP Certificate	<p>Note The private key must be in .pem format.</p> <p>Signing Authentication Requests</p> <p>If you want the appliance to sign the SAML authentication requests:</p> <ol style="list-style-type: none"> Upload the certificate and the associated private key. Enter the passphrase for the private key. Select Sign Request. <p>Decrypt Encrypted Assertions</p> <p>If you plan to configure your identity provider to encrypt SAML assertions:</p> <ol style="list-style-type: none"> Upload the certificate and the associated private key. Enter the passphrase for the private key.
Sign Assertions	If you want the identity provider to sign the SAML assertions, select Sign Assertions . If you select this option, you must add the identity provider's certificate to the appliance. See Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 530 .
Organization Details	Enter the details of your organization. Identity provider uses this information in the error logs.
Technical Contact	Enter the email address of the technical contact. Identity provider uses this information in the error logs.

Step 5 Click **Submit**.

Step 6 Note down the service provider metadata (Entity ID and Assertion Customer URL) displayed on the SSO Settings page and the Name ID Format displayed on the Service Provider Settings page. You will need these details while configuring the service provider settings on the identity provider.

Optionally, you can export the metadata as a file. Click **Export Metadata** and save the metadata file. Some identity providers allow you to load service provider details from a metadata file.

What to do next

Configure the identity provider to communicate with your appliance. See [Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 530](#).

Configuring the Identity Provider to Communicate with Cisco Security Management Appliance

Before you begin

Make sure that you have:

- Configured your appliance as a service provider. See [Configure Cisco Content Security Management Appliance as a Service Provider, on page 528](#).
- Copied the service provider metadata details or exported the metadata file. See [Configure Cisco Content Security Management Appliance as a Service Provider, on page 528](#).

Step 1 On the identity provider, do one of the following:

- Manually configure the details of the service provider (your appliance).
- If your identity provider allows you to load the service provider details from a metadata file, import the metadata file.

If you have configured your appliance to sign the SAML authentication requests or you plan to encrypt SAML assertions, make sure that you add the relevant certificate to the identity provider.

For identity provider-specific instructions, see:

- [Configure AD FS to Communicate with Cisco Security Management Appliance, on page 531](#).
- [Configure Azure AD to Communicate with Cisco Security Management Appliance, on page 531](#).
- [Configure Duo Access Gateway to Communicate with Cisco Security Management Appliance, on page 532](#).

Step 2 Note down the identity provider metadata or export the metadata as a file.

What to do next

Configure the identity provider settings on your appliance. See [Configuring the Identity Provider to Communicate with Cisco Security Management Appliance, on page 530](#).

Configure AD FS to Communicate with Cisco Security Management Appliance

The following are the high level tasks you need to perform to configure AD FS (2.0 and later) to communicate with your appliance. For complete and detailed instructions, see *Microsoft documentation*.

- Add the service provider's (appliance's) Assertion Consumer URL as a relaying party.
- Enter the service provider's (appliance's) Entity ID under Relaying Party Trusts > Properties > Identifiers > Relaying Party Identifier. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.
- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) in .cer format under Relaying Party Trusts > Properties > Signature.
- If you plan to configure AD FS to send encrypted SAML assertions, upload the service provider's (appliance's) certificate in .cer format under Relaying Party Trusts > Properties > Encryption.
- Set the Secure-hash Algorithm to SHA-1 under Relaying Party Trusts > Properties > Advanced.
- Add a custom rule to include SPNameQualifier in the response. The following is a sample custom rule:


```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer=
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```
- Edit the Claim Rule and add an Issuance Transform Rule to send the LDAP attribute for email address as an outgoing claim type (email address). Also ensure that you add an Issuance Transform Rule to send the LDAP attribute for group attribute as an outgoing claim type (unspecified groups).

Configure Azure AD to Communicate with Cisco Security Management Appliance

The following are the high level tasks you need to perform to Azure AD to communicate with your appliance. For complete and detailed instructions, see *Microsoft Azure AD Documentation*.

- Add the service provider's (appliance's) Assertion Consumer URL as the service provider identifier that receives and processes SAML assertions.
- Enter the service provider's (appliance's) Entity ID in the Azure Portal under Enterprise Application > New Application > Non-gallery application > Single Sign-On > Basic SAML Configuration. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.
- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) under SAML Signing Certificate section (Enterprise Application > New Application > Non-gallery application > Single Sign-On > SAML Signing Certificate).
- Configure a Group Claim under User Attributes and Claims section (Enterprise Application > New Application > Non-gallery application > Single Sign-On > User Attributes and Claims) and add the group attribute.

- Add users and groups under Enterprise Application > New Application > Non-gallery application > Users & Groups) to allow users to log in to the application based on the SAML assertion or response.

Configure Duo Access Gateway to Communicate with Cisco Security Management Appliance

The following are the high level tasks you need to perform to Duo Access Gateway to communicate with your appliance. For complete and detailed instructions, see *Duo Security Documentation*.


- Add the service provider's (appliance's) Assertion Consumer URL as the service provider endpoint that receives and processes SAML assertions.
- Enter the service provider's (appliance's) Entity ID under Duo Admin Panel > Applications > Protect an Application > SAML Service Provider. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.
- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) in .cer format when you configure the authentication source on the Duo Access Gateway.
- If you plan to configure Duo to send encrypted SAML assertions, upload the service provider's (appliance's) certificate in .cer format when you configure the authentication source on the Duo Access Gateway.
- Select the NameID format as "unspecified" under Duo Admin Panel > Applications > Protect an Application > SAML Service Provider > SAML Response.
- Set the Secure-hash Algorithm to SHA-256 under Duo Admin Panel > Applications > Protect an Application > SAML Service Provider > SAML Response.
- Save the SAML - Service Provider Setting as a configuration file on the Duo Admin Panel and import the configuration file as a SAML application on the Duo Access Gateway.

Configure Identity Provider Settings on Cisco Content Security Management Appliance

Before you begin

Make sure that you have:

- Configured the identity provider to communicate with your appliance. See [Configuring the Identity Provider to Communicate with Cisco Security Management Appliance](#), on page 530.
- Copied the identity provider metadata details or the exported metadata file.

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

Step 2 Choose **Management Appliance > System Administration > SAML**.

Step 3 Under the Identity Provider section, click **Add Identity Provider**.

Step 4 Enter the following details:

Field	Description
Profile Name	Enter a name for the identity provider profile.

Field	Description
Configuration Settings (Manually Configure Identity Provider Settings)	
Entity ID	Enter a globally unique name for the identity provider. The format of the identity provider Entity ID is typically a URI.
SSO URL	Specify the URL to which the service provider must send the SAML authentication requests.
Certificate	If the identity provider signs the SAML assertion, you must upload the identity provider's signing certificate.
Configuration Settings (Importing Identity Provider Metadata)	
Import IDP Metadata	Click Import Metadata and select the metadata file.

Step 5 Submit and commit your changes.

What to do next

[Enable SAML Authentication, on page 533](#)

Enable SAML Authentication

You can enable Single Sign On using SAML to authenticate users and assign groups of users to Cisco rules.

Before you begin

Make sure that you have configured the SAML profiles with Service Provider and Identity Provider settings. See [How to Configure SSO on your Cisco Security Management Appliance, on page 527](#).

Step 1 Navigate to **Management Appliances > System Administration > Users**.

Step 2 Scroll down to the **External Authentication** section.

Step 3 Click **Enable**.

Step 4 Select the **Enable External Authentication** check box.

Step 5 Select **SAML** as the authentication type from the drop-down list.

Step 6 **(Optional)** In the **External Authentication Attribute Name Map** field, enter the attribute name to search from the Group Mapping.

The Attribute Name depends on the attributes that you configure for the Identity Provider. The appliance will search for matching entries of the Attribute Name in the **Group Mapping** field. This is optional and if you do not configure, the appliance will search for matching entries of all attributes present in the Group Mapping field.

Step 7 In the **Group Mapping** field, enter the group name attribute as defined in the SAML directory based on the predefined or custom user role. You can click **Add Row** to add multiple role mappings.

The Group Mapping must contain a group attribute. You can add 'Unspecified Groups' attribute to authenticate SAML assertions or response.

For more information on types of user roles, see [Users Page , on page 412](#).

Step 8 Submit and commit your changes.

What to do next

After you enable SAML external authentication, you can use the **Use Single Sign On** link on the login page of the appliance and enter the username to log in to the appliance.

How to Configure SSO for Spam Quarantine

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 534
Step 2	Configure your appliance as a service provider.	Configure Cisco Content Security Management Appliance as a Service Provider, on page 535
Step 3	[On IDP] Configure the identity provider to work with your appliance.	Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance
Step 4	Configure identity provider settings on your appliance.	Configure Identity Provider Settings on Cisco Content Security Management Appliance, on page 538
Step 5	Enable SSO for Spam Quarantine on your appliance.	Enable SSO for Spam Quarantine, on page 539
Step 6	Notify the end users about the new authentication mechanism.	


Prerequisites

- Verify whether the identity provider used by your organization is supported by Cisco Content Security Management Appliance. The following are the supported identity providers:
 - Microsoft Active Directory Federation Services (AD FS) 2.0
 - Ping Identity PingFederate 7.2
 - Cisco Web Security Appliance 9.1
- Obtain the following certificates that are required to secure the communication between your appliance and the identity provider:
 - If you want your appliance to sign SAML authentication requests or if you want your identity provider to encrypt SAML assertions, obtain a self signed certificate or a certificate from a trusted CA and the associated private key.
 - If you want the identity provider to sign SAML assertions, obtain the identity provider's certificate. Your appliance will use this certificate to verify the signed SAML assertions.

Configure Cisco Content Security Management Appliance as a Service Provider

Before you begin

Review the [Prerequisites](#), on page 534.

- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > SAML**.
- Step 3** Under the Service Provider section, click **Add Service Provider**.
- Step 4** Enter the following details:

Field	Description
Profile Name	Enter a name for the service provider profile.
Configuration Settings	
Entity ID	Enter a globally unique name for the service provider (in this case, your appliance). The format of the service provider Entity ID is typically a URI.
Name ID Format	The format that the identity provider should use to specify the user in the SAML assertion. This field is not configurable. You will need this value while configuring the identity provider.
Assertion Consumer URL	The URL to which the identity provider should send the SAML assertion after authentication has successfully completed. In this case, this is the URL to your spam quarantine. This field is not configurable. You will need this value while configuring the identity provider.
SP Certificate	<p>Note The private key must be in .pem format.</p> <p>Signing Authentication Requests</p> <p>If you want the appliance to sign the SAML authentication requests:</p> <ol style="list-style-type: none"> Upload the certificate and the associated private key. Enter the passphrase for the private key. Select Sign Request. <p>Decrypt Encrypted Assertions</p> <p>If you plan to configure your identity provider to encrypt SAML assertions:</p> <ol style="list-style-type: none"> Upload the certificate and the associated private key. Enter the passphrase for the private key.

Field	Description
Sign Assertions	If you want the identity provider to sign the SAML assertions, select Sign Assertions . If you select this option, you must add the identity provider's certificate to the appliance. See Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance, on page 536 .
Organization Details	Enter the details of your organization. Identity provider uses this information in the error logs.
Technical Contact	Enter the email address of the technical contact. Identity provider uses this information in the error logs.

Step 5 Click **Submit**.

Step 6 Note down the service provider metadata (Entity ID and Assertion Customer URL) displayed on the SSO Settings page and the Name ID Format displayed on the Service Provider Settings page. You will need these details while configuring the service provider settings on the identity provider.

Optionally, you can export the metadata as a file. Click **Export Metadata** and save the metadata file. Some identity providers allow you to load service provider details from a metadata file.

What to do next

Configure the identity provider to communicate with your appliance. See [Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance, on page 536](#).

Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance

Before you begin

Make sure that you have:

- Configured your appliance as a service provider. See [Configure Cisco Content Security Management Appliance as a Service Provider, on page 535](#).
- Copied the service provider metadata details or exported the metadata file. See [Configure Cisco Content Security Management Appliance as a Service Provider, on page 535](#).

Step 1 On the identity provider, do one of the following:

- Manually configure the details of the service provider (your appliance).
- If your identity provider allows you to load the service provider details from a metadata file, import the metadata file.

If you have configured your appliance to sign the SAML authentication requests or you plan to encrypt SAML assertions, make sure that you add the relevant certificate to the identity provider.

For identity provider-specific instructions, see:

- [Configure AD FS 2.0 to Communicate with Cisco Content Security Management Appliance, on page 537](#)
- [Configure PingFederate 7.2 to Communicate with Cisco Content Security Management Appliance, on page 537](#)
- **Configuring the Appliance as an Identity Provider** section in the *User Guide for AsyncOS for Cisco Web Security Appliances* <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html>

Step 2 Note down the identity provider metadata or export the metadata as a file.

What to do next

Configure the identity provider settings on your appliance. See [Configure Identity Provider Settings on Cisco Content Security Management Appliance, on page 538](#).

Configure AD FS 2.0 to Communicate with Cisco Content Security Management Appliance

The following are the high level tasks you need to perform to configure AD FS 2.0 to communicate with your appliance. For complete and detailed instructions, see Microsoft documentation.

- Add the service provider's (appliance's) Assertion Consumer URL as a relaying party.
- Enter the service provider's (appliance's) Entity ID under Relaying Party Trusts > Properties > Identifiers > Relaying Party Identifier. Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.
- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate (used to sign authentication requests) in .cer format under Relaying Party Trusts > Properties > Signature.
- If you plan to configure AD FS to send encrypted SAML assertions, upload the service provider's (appliance's) certificate in .cer format under Relaying Party Trusts > Properties > Encryption.
- Set the Secure-hash Algorithm to SHA-1 under Relaying Party Trusts > Properties > Advanced.
- Edit the Claim Rule and add an Issuance Transform Rule to send the LDAP attribute for email address as an outgoing claim type (email address).
- Add a custom rule to include SPNameQualifier in the response. The following is a sample custom rule:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<appliance-hostname>.83");
```

Configure PingFederate 7.2 to Communicate with Cisco Content Security Management Appliance

The following are the high level tasks you need to perform to configure PingFederate 7.2 to communicate with your appliance. For complete and detailed instructions, see Ping Identity documentation.

- Add your service provider's (appliance's) Assertion Consumer URL as an endpoint under protocol settings.
- Enter the service provider's (appliance's) Entity ID under SP Connection > General Info > Partner's Entity ID (Connection ID). Make sure that this value is same as the Entity ID value in the Service Provider settings on your appliance.


- If you have configured your service provider (appliance) to send signed SAML authentication requests, upload the service provider's certificate under Signature Verification section (SP Connection > Credentials > Signature Verification > Signature Verification Certificate).
- If you plan to configure PingFederate to send encrypted SAML assertions, upload the service provider's (appliance's) certificate under Signature Verification section (SP Connection > Credentials > Signature Verification > Select XML Encryption Certificate).
- Edit Attribute Contract to send the LDAP attribute- email address (Attribute Sources & User Lookup > Attribute Contract Fulfillment).

Configure Identity Provider Settings on Cisco Content Security Management Appliance

Before you begin

Make sure that you have:

- Configured the identity provider to communicate with your appliance. See [Configure the Identity Provider to Communicate with Cisco Content Security Management Appliance, on page 536](#).
- Copied the identity provider metadata details or the exported metadata file.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > System Administration > SAML**.
- Step 3** Under the Identity Provider section, click **Add Identity Provider**.
- Step 4** Enter the following details:

Field	Description
Profile Name	Enter a name for the identity provider profile.
Configuration Settings (Manually Configure Identity Provider Settings)	
Entity ID	Enter a globally unique name for the identity provider. The format of the identity provider Entity ID is typically a URI.
SSO URL	Specify the URL to which the service provider must send the SAML authentication requests.
Certificate	If the identity provider signs the SAML assertion, you must upload the identity provider's signing certificate.
Configuration Settings (Importing Identity Provider Metadata)	
Import IDP Metadata	Click Import Metadata and select the metadata file.

- Step 5** Submit and commit your changes.
-

What to do next


[Enable SSO for Spam Quarantine, on page 539](#)

Enable SSO for Spam Quarantine

Before you begin

Make sure that you have:

- Configured all the settings on **Management Appliance > System Administration > SAML** page.
- Enabled Spam Quarantine. See [Spam Quarantine, on page 267](#).

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Spam Quarantine**.
- Step 3** Click **Edit Settings** and scroll down to the End-User Quarantine Access section.
- Step 4** Make sure that you have enabled End-User Quarantine Access.
- Step 5** Set the End-User Authentication method to **SAML2.0**.
- Step 6** (Optional) Specify whether to display message bodies before messages are released.
- Step 7** Submit and commit your changes.
-

What to do next

Notify the end users about the new authentication mechanism.

Configuring OpenID Connect 1.0 on Cisco Content Security Management for AsyncOS APIs

- [Overview](#) , on page 539
- [Workflow](#) , on page 540
- [Sample Access Token](#), on page 540
- [Prerequisites](#) , on page 541
- [Configuring OpenID Connect on Appliance](#), on page 541
- [Configuring OpenID Connect on Appliance using CLI](#), on page 542

Overview

The Cisco Content Security Management Appliance supports integration with applications or clients that use Identity Providers (IDPs) with OpenID Connect 1.0 authentication to connect seamlessly with AsyncOS APIs available in your appliance. Currently, your appliance has been certified with OpenID Connect using Microsoft AD FS only.

Workflow

In the following workflow, AD FS is used as an identity provider, external application as a client, and your appliance as a resource provider.

Steps:

1. In the following workflow, AD FS is used as an identity provider, external application as a client, and your appliance as a resource provider, see [Configuring OpenID Connect on Appliance, on page 541](#).
2. [One-time activity] The appliance fetches the OpenID Connect configuration metadata and the required keys to validate the access token based on the configuration done in step1.
3. Obtain the access token after you authenticate the external application with AD FS. For more information on how to authenticate and receive the access token, see your Authentication Provider or Identity Provider documentation.
4. Send the API request along with the access token to the appliance.
5. The appliance validates the access token in the API request using the key set retrieved from step2.
6. The appliance validates the required claim (issuer, audience) in the access token.
7. The appliance uses the role claim value to authorize and allocate the user role privileges to access the AsyncOS APIs.
8. The appliance provides an appropriate response for the AsyncOS API request.

Sample Access Token

The following is the format of a sample access token:

Header

alg:RSA256

typ:JWT

[...]

Payload

claim:aud: CiscoEmailAPICaller

claim:iss:<http://adfserver/adfs/services/trust>

claim:iat: 1594712147

claim:exp: 1594712807

claim:CustomOrgIdentifier: MyCustomOrgId

claim:LastName: Fernandes

claim:FirstName: Erik

claim:Email: [http://erik.fernandes@customorg.com](mailto:erik.fernandes@customorg.com)

claim:Role: LogCollector

claim:Role: ReadOnly

[.....]

The appliance supports the validation of access tokens signed by the following algorithms only:

- RSA256
- RSA384
- RSA512

Prerequisites

Make sure that you have met the following prerequisites before you configure your appliance with OpenID Connect:

- The authentication provider used by your organization is supported by the appliance.
- The application can authenticate with the authentication provider and retrieve the access token.
- The appliance can connect to the authentication provider over HTTPs to fetch the OpenID Connect metadata configuration.

Configuring OpenID Connect on Appliance

Before you begin

Make sure that you have the following:

- A valid access token issued by the authentication provider (based on your authentication provider setup).
- The access token must include the role information to allow the appliance to perform the required authorization checks.

Step 1 Click **System Administration > OpenID Connect** .

Step 2 Click **Edit Settings**

Step 3 Enter the required parameters described in the following table to configure OpenID Connect:

OpenID Connect Parameters	Description
Identity Provider Metadata URL	Enter the identity provider URL used to fetch the OpenID Connect configuration metadata. The metadata is used to validate the access token. The following is an example of an identity provider URL - https://example.com/adfs/.well-known/openid-configuration
Issuer	Enter the value of the issuer of the access token. Note The value must match the issuer claim value of the access token when validating the access token. The following is an example of an issuer - http://example.com/adfs/services/trust

OpenID Connect Parameters	Description
Audience	Enter the value of the audience that must match the audience claim value of the access token. Note Click Add Row if you want to add more than one audience value.
Claim Name	Enter the name of the claim in the access token, which contains the user role information. The claim name is used to retrieve the role information from the access token.
Identity Provider to Appliance Role Mapping	Enter a user group role defined in the Identity Provider server and choose a corresponding local user role configured in the appliance to map both roles. Note Click Add Row if you want to add more than one role mapping record.

Step 4 Submit and commit your changes.

What to do next

Include the access token in the Authorization Bearer header of the AsyncOS API call and send the API request.

The following is an example of invoking an AsyncOS API with the access token in the Authorization Bearer header of the API.

```
curl --location --request
GET 'https://sma.com/sma/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'
--header 'Authorization: Bearer <add access_token here>'
```

Configuring OpenID Connect on Appliance using CLI

Use the **oidconfig** command to perform the following tasks:

- Configure OpenID Connect on your email gateway for AsyncOS APIs.
- Delete OpenID Connect configuration settings on your email gateway.

Customizing Your View

- [Using Favorite Pages](#) , on page 542
- [Setting Preferences](#) , on page 543
- [General Settings](#), on page 544

Using Favorite Pages

(Locally-authenticated administrative users only.) You can create a quick-access list of the pages you use most.

To	Do This
Add pages to your favorites list	Navigate to the page to add, then choose Add This Page To My Favorites from the My Favorites menu near the top right corner of the window. No commit is necessary for changes to My Favorites.
Reorder favorites	Choose My Favorites > View All My Favorites and drag favorites into the desired order.
Edit favorite page, name, or description	Choose My Favorites > View All My Favorites and click the name of the favorite to edit.
Delete favorites	Choose My Favorites > View All My Favorites and delete favorites.
Go to a favorite page	Choose a page from the My Favorites menu near the top right corner of the window.
Return to the main interface	Choose any favorite, or click the Return to previous page at the bottom of the page.

Setting Preferences

Administrative users configured on the Security Management appliance

Locally-authenticated users can choose the following preferences, which apply each time the user logs in to the Security Management appliance:

- Language (applies to the GUI)
- Landing page (the page displayed after login)
- Default time range for report pages (available options are a subset of the time ranges available for Email and Web reporting pages)
- Number of rows visible in tables on report pages

Exact options depend on the user role.

To set these preferences, choose **Options > Preferences**. (The Options menu is at the top right side of the GUI window.) Submit your changes when done. Commit is not required.



Tip To return to the page you were viewing before you accessed the Preferences page, click the **Return to previous page** link at the bottom of the page.

Externally authenticated users


Externally authenticated users can choose the display language directly in the Options menu.

General Settings

- [Improving Web Interface Rendering](#) , on page 544
- [Monitoring Web Usage Analytics](#), on page 544

Monitoring Web Usage Analytics

Usage Analytics is used to provide insight into your site activity data for analytical statistics. If Usage Analytics is enabled, the appliance collects the feature usage data of the appliance on the new web interface. The usage statistics are used to analyze and provide insight to improve the user experience of the appliance.


-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 2** Choose **Management Appliance > System Administration > General Settings**.
 - Step 3** Click on **Edit Settings**.
 - Step 4** Select the **Enable** check box in the Usage Analytics field.
 - Step 5** Submit and commit your changes.
-

Improving Web Interface Rendering

For better web interface rendering, Cisco recommends that you enable Internet Explorer Compatibility Mode Override.



Note If enabling this feature is against your organizational policy, you may disable this feature.

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
 - Step 2** Choose **Management Appliance > System Administration > General Settings**.
 - Step 3** Click on **Edit Settings**.
 - Step 4** Select the **Enable** check box in the Override IE Compatibility Mode field.
 - Step 5** Submit and commit your changes.
-

Restarting and Viewing Status of Services Enabled on Appliance

You can use the `diagnostic > services` sub command in the CLI to:

- Restart the services enabled on your appliance without having to reboot your appliance.
- View the status of the services enabled on your appliance.

Example: Viewing Status of Reporting Service

In the following example, the `services` command is used to view the status of the reporting service enabled on your appliance.

```
mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.

[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- API_SERVER - API Server
[]> reporting

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

Reporting has been up for 28d 20h 45m 35s.
```

Example: Restarting the Message Tracking Service

In the following example, the `services` command is used to restart the message tracking service enabled on your appliance.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.

[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- API_SERVER - API Server
[]> tracking

Choose the operation you want to perform:
- RESTART - Restart the service
```

```
- STATUS - View status of the service
[ ]> restart
```

Managing Lists of Certificate Authorities

The appliance uses stored trusted certificate authorities to verify a certificate from a remote domain to establish the credentials of the domain. You can configure the security management appliance to use the following trusted certificate authorities:

- System list- The appliance has a pre-installed list of trusted certificate authorities. This is called the system list.
- Custom list- You can customize a list of trusted certificate authorities, and then import the custom list into the appliance.



Note You can use either the system list or the customized list, or both to verify certificate from a remote domain.

Manage the lists using the **Network > Certificates > Edit Certificate Authorities** page in the GUI or the **certconfig > certauthority** command in the CLI.

On the **Network > Certificates > Edit Certificate Authorities** page, you can perform the following tasks:

- Choose whether or not to use the system list. You can enable or disable the system list. For more information, see [Disabling the System Certificate Authority List, on page 546](#).
- Choose whether or not to use a custom certificate authority list. You can enable the appliance to use a custom list and then import the list from a text file. For more information, see [Importing a Custom Certificate Authority List, on page 547](#).
- Export the list of certificate authorities. You can export either the system or customized list of certificate authorities to a location in your local drive. For more information, see [Exporting a Certificate Authority List, on page 547](#).

On the **Network > Certificates > Manage Trusted Root Certificates** page, you can perform the following tasks:

- View the custom and system list of certificates. For more information, see [Displaying Trust Root Certificate, on page 548](#).
- Delete an existing certificate. You can delete a custom certificate that you have imported. For more information, see [Deleting Custom Certificate, on page 548](#).

Disabling the System Certificate Authority List

The pre-installed system certificate authorities list cannot be removed from the appliance, but you can enable or disable it. You can disable it to allow the appliance to only use your list to verify certificates from remote hosts.

Procedure

	Command or Action	Purpose
Step 1	Navigate to the Network > Certificates page.	
Step 2	Click Edit Settings in the Certificate Authorities section.	
Step 3	Click Disable for the System List.	
Step 4	Submit and commit your changes.	

Importing a Custom Certificate Authority List

You can create a custom list of trusted certificate authorities and import it onto the appliance. The file must be in the PEM format and include certificates for the certificate authorities that you want the appliance to trust.

-
- Step 1** Click **Network > Certificate**.
 - Step 2** Click **Edit Settings**.
 - Step 3** Choose the **Enable** radio button.
 - Step 4** Click **Choose File** in Custom List.
 - Step 5** Browse to the location where the certificate resides, and click **Ok**.
 - Step 6** [Optional] Select the FQDN Validation check box to allow the email gateway to check whether the 'Common Name', 'SAN: DNS Name' fields, or both present in the certificate, are in the FQDN format.
 - Step 7** Click **Submit**.

Note Below checks will done on CA import,

- Expiry
- Duplication
- CA flag is present and Set to "True"
- Root Certificate Authority is present if importing Intermediate Certificate Authority is imported.

Exporting a Certificate Authority List

If you want to use only a subset of the trusted certificate authorities in the system or edit an existing custom list.



Note You can export the custom list to a .txt file, edit to add or remove certificate authorities, and then import the file back onto the appliance as a custom list.

-
- Step 1** Click **Network > Certificate**.
- Step 2** Click **Edit Settings**.
The Edit Settings list the custom and Cisco trusted root certificates.
- Step 3** Click the Certificate name.
- Step 4** Click **Export** to export the certificate.
-

Displaying Trust Root Certificate

- Step 1** Click **Network > Certificate**.
- Step 2** Click **Manage Trusted Root Certificates**.
The Manage Trusted Root Certificates lists the custom and Cisco trusted root certificates.
- Step 3** Check the **Override Trust** check box to override the trust.
- Step 4** Click **Submit**.
In the Manage Trusted Root Certificates page, you can click on Download Certificate to download and store the certificate to your local machine.
-

Deleting Custom Certificate

- Step 1** Click **Network > Certificate**.
- Step 2** Click **Manage Trusted Root Certificates**.
The Manage Trusted Root Certificates lists the custom certificates.
- Step 3** Click **Delete** to delete a custom trusted root certificate.
- Step 4** Click **Submit**.
-

Configuring CRL Sources

The Secure Email and Web Manager checks a list of revoked certificates called a Certificate Revocation List (CRL) as part of its certificate verification to ensure that the user's certificate has not been revoked. You need to keep an up-to-date version of this list on a server, and the Secure Email and Web Manager downloads it on a schedule you create. You can manually update the list too.

Related Topics

- [Configuring CRL Sources using GUI, on page 549](#)
- [Configuring Global Settings for CRL Sources, on page 550](#)

- [Configuring CRL Sources using CLI, on page 550](#)

Configuring CRL Sources using GUI

You can configure the CRL sources to enable or disable checking the list of revoked certificates. You can add, update, and delete the CRL sources.

To configure the CRL sources, perform the following steps:

Step 1 Click **Network > CRL Sources**.

Step 2 Click **Add CRL Source** to add a new CRL source.

The **Add CRL (Certificate Revocation Lists) Source** window is displayed.

Step 3 Enter the required parameters described in the following table to add a CRL source on Secure Email and Web Manager.

Parameter	Description
CRL File Name	Enter the name of the CRL source file.
CRL File Type	Enter the type of CRL source file. You can select ASN.1 (Abstract syntax notation 1) or PEM (Privacy Enhanced Mail) CRL file type.
Primary source URL to download a CRL file from	Enter the URL for the primary source of the file, including the filename. For example, https://crl.example.com/certs.crl
Secondary source URL to use when the primary source is not available (optional)	Enter the URL for the secondary source of the file, including the filename. This field is optional.
Enable Scheduled auto update of CRL file	Enter the schedule to download the CRL source file. Select Enable Scheduled auto update of CRL file to enable scheduled auto-update. You can select the Daily, Weekly, or Monthly option and specify the time (in 24-hour format) when the download must happen.
Test Source	Click Test CRL Source to test whether the CRL source file is updated successfully. Note The CRL source file is not downloaded in the database. When you click this button it tests if the CRL source file is updated successfully.

Step 4 Submit and commit your changes.

What to do next

You can update and delete the CRL source.

- Select the CRL source and click **Update** to update the CRL source manually.

- Select the CRL source and click the **delete icon** to delete the CRL source. Click **Clear All CRL Sources** to delete all the CRL sources.

Configuring Global Settings for CRL Sources

You can configure the global settings for CRL sources to enable or disable the CRL check for the following connections:

- Inbound SMTP TLS
- Outbound SMTP TLS
- Web Interface

To configure global settings for CRL sources, perform the following steps:

-
- Step 1** Click **Network > CRL Sources**.
- Step 2** Click **Edit Settings** in the **Global Settings for CRL Sources** section of the **CRL Sources** window.
- Step 3** Check or uncheck the following check boxes to enable or disable the options provided:
- **CRL check for inbound SMTP TLS**
 - **CRL check for outbound SMTP TLS**
 - **CRL check for Web Interface**
- Check the **Global Settings** check box to enable all the options.
- Step 4** Submit and commit your changes.
-

Configuring CRL Sources using CLI

You can use the `certconfig > CRL` subcommand to configure CRL sources using CLI.

When you execute the command, you can perform the operations mentioned in the table below:

Subcommand	Purpose
NEW	Adds a new CRL source.
EDIT	Modifies the existing CRL source.
DELETE	Removes the CRL source.
PRINT	Displays all the CRL sources.
UPDATE	Updates the CRL sources manually.

Subcommand	Purpose
SETUP	Configures the global settings for the CRL sources. You can enable or disable the CRL check for the following connections: <ul style="list-style-type: none"> • Inbound SMTP TLS • Outbound SMTP TLS • Web Interface

Example 1:

You can use the `SETUP` subcommand to enable CRL check for Web Interface as shown in the following example:

```
mail3.example.com> certconfig

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

Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Disabled

There are currently 1 CRL sources configured.

Choose the operation you want to perform:
- NEW - Create a new CRL source
- EDIT - Modify a CRL source
- DELETE - Remove a CRL source
- PRINT - Display all CRL sources
- UPDATE - Manually update a CRL file
- SETUP - Change global settings
[]> setup

Do you want to enable CRL check for inbound SMTP TLS? [N]> n

Do you want to enable CRL check for outbound SMTP TLS? [N]> n

Do you want to enable CRL check for Web Interface? [N]> y

Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Enabled

There are currently 1 CRL sources configured.
```

Example 2:

You can use the `PRINT` subcommand to display all the CRL sources as shown in the following example:

```
mail3.example.com> certconfig

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

```

- CRL - Manage Certificate Revocation Lists
[]> CRL

Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Disabled
There are currently 1 CRL sources configured.

Choose the operation you want to perform:
- NEW - Create a new CRL source
- EDIT - Modify a CRL source
- DELETE - Remove a CRL source
- PRINT - Display all CRL sources
- UPDATE - Manually update a CRL file
- SETUP - Change global settings

[]> PRINT
Currently configured CRL sources (disabled sources are marked with *):
1. crl16: http://crl.example.com/certs.crl.pem
Certificate Revocation List Summary
Inbound SMTP TLS: Disabled
Outbound SMTP TLS: Disabled
Web Interface: Disabled
There are currently 1 CRL sources configured.
Choose the operation you want to perform:
- NEW - Create a new CRL source
- EDIT - Modify a CRL source
- DELETE - Remove a CRL source
- PRINT - Display all CRL sources
- UPDATE - Manually update a CRL file
- SETUP - Change global settings

```

Receiving and Delivering Messages with Internationalised Domain Names (IDNs)

The Cisco Secure Email and Web Manager can receive and deliver messages with email addresses that contain IDN domains.

Currently, your email gateway provides support of IDN domains for the following languages only:

Indian Regional Languages: Hindi, Tamil, Telugu, Kannada, Marati, Punjabi, Malayalam, Bengali, Gujarati, Urdu, Assamese, Nepali, Bangla, Bodo, Dogri, Kashmiri, Konkani, Maithili, Manipuri, Oriya, Sanskrit, Santali, Sindhi, and Tulu.

European and Asian Languages: French, Russian, Japanese, German, Ukrainian, Korean, Spanish, Italian, Chinese, Dutch, Thai, Arabic, and Kazakh.

Related Topics

- [Prerequisites IDN, on page 553](#)
- [Features Configurable using IDN Domains in Cisco Secure Email and Web Manager, on page 553](#)

Prerequisites IDN

Make sure you have met the following prerequisites before you use the Internationalised Domain Names (IDN) feature:

- All incoming messages must have IDNs encoded in UTF-8.

For Example: An MTA that sends messages to the email gateway must support IDNs and make sure the domains in the messages are in the UTF-8 format.

- All outgoing messages must have IDNs encoded in UTF-8, and the destination server must accept and support IDNs accordingly.

For Example: An MTA that accepts messages from the email gateway must support IDNs and domains encoded in the UTF-8 format.

- In all applicable DNS records, IDNs must be configured using the Punycode format

For Example: When you configure an MX record for an IDN, the domain in the DNS record must be in the Punycode format.

Features Configurable using IDN Domains in Cisco Secure Email and Web Manager

For this release, you can only configure the following features using IDN domains in your Cisco Secure Email and Web Manager :

- **SMTP Routes Configuration Settings:**

- Add or edit IDN domains.
- Export or import SMTP routes using IDN domains.

- **DNS Configuration Settings:** Add or edit the DNS server using IDN domains.

- **Reporting Configuration Settings:** View IDN data - usernames, email addresses, and domains) in the reports.

- **Message Tracking Configuration Settings:** View IDN data- usernames, email addresses, and domains) in message tracking.

- **Policy, Virus, and Outbreak Quarantine Configuration Settings:**

- View messages with IDN domains that may be transmitting malware, as determined by the anti-virus engine.
- View messages with IDN domains caught by Outbreak Filters as potentially being spam or malware.
- View messages with IDN domains caught by message filters, content filters, and DLP message actions.

- **Spam Quarantine Configuration Settings:**

- View messages with IDN domains detected as spam or suspected spam.
- Add email addresses with IDN domains to the safelist and blocklist categories.

- **End User Quarantine-** IDN support with Authentication Mode as NONE. Other auth modes are not supported in this phase.

FQDN

A fully qualified domain name (FQDN) is the complete domain name for a specific computer, or host, on the internet. For a X.509 certificate, the FQDN validation validates the common name field (CN) of that certificate's subject distinguished name and the subjectAltName extension of type dNSName (SAN:dNSName). AsyncOS validates the domain name and the certificates for the common name and SAN:dNSName in its fields. Preferably the SAN:dNSName names are used. Examples of valid FQDN include example.com, *.example.com.

The criteria for FQDN compliance includes:

- Either the CN or the SAN:dNSName should be present in the certificate and AsyncOS mandates that either one should be FQDN compliant.
- Both the CN and SAN:dNSName are present in the certificate and AsyncOS mandates that both should be FQDN compliant.

The variants include:

- [Validation on Peer Certificate, on page 554](#)
- [Custom CA Validation, on page 555](#)
- [Appliance Certificate Validation, on page 555](#)

When you perform an add or import of the appliance certificate, Cisco Secure Email and Web Manager performs FQDN validation on the certificate when its FQDN validation is enabled and during the peer certificate validation of the server. All detailed logging is tracked in the Cisco Secure Email and Web Manager system.current or gui.current log files. However; Cisco Secure Email and Web manager does not enable you to import a certificate that does not have a common name (CN) and has an alternate subject name without a critical extension.

Validation on Peer Certificate

AsyncOS provides a common configuration to control FQDN validation for all services under SSL configuration, for example TLS. However, you must enable the FQDN service manually.

- [Validation on Peer Certificate Using the GUI, on page 554](#)
- [Validation on Peer Certificate Using the CLI, on page 555](#)

Validation on Peer Certificate Using the GUI

-
- Step 1** Go to **System Administration > SSL Configuration** page.
 - Step 2** Click **Edit Settings**.
 - Step 3** Check the **Enable** checkbox listed with Peer Certificate FQDN Validation.

Step 4 Click **Submit**.

Validation on Peer Certificate Using the CLI

You must enter the `sslconfig` command to perform a validation on peer certificate.

Before you begin

```
prompt> sslconfig
```

Disabling SSLv3 is recommended for best security.

Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:

- VERSIONS - Enable or disable SSL/TLS versions
 - PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater and LDAP.
-

Custom CA Validation

AsyncOS enables you to perform a FQDN validation when you import the custom certificate authority into the appliance. You must enable the validation manually.

Step 1 Enter the command `CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT`

Enter in the command-line interface the `CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT` command

Step 2 Enter the filename of the file you want to import.

Enter the name of the file on machine "appliance" to import:

```
[> filename.pem
```

Step 3 Confirm if you want to check for FQDN.

```
Do you want to check if Common Name is in Fully Qualified Domain Name (FQDN) format ? [N]> y
```

Appliance Certificate Validation

AsyncOS enables you to perform a FQDN validation when you import the appliance certificate into the appliance. You must enable the validation manually.

Step 1 Enter the `CERTCONFIG > CERTIFICATE > SETUP` command.

```
Prompt> CERTCONFIG > CERTIFICATE > SETUP >
```

Step 2 Enter if you want the intermediate certificate.

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

Step 3 Enter if you want to check for FQDN.

```
Do you want to check if Common Name is in Fully Qualified Domain Name(FQDN) format ? [N]> y
```

X.509 Certificate

X.509 is an International Telecommunication Union (ITU) standard that defines the format of public key certificates. An X.509 certificate binds an identity to a public key using a digital signature.

The criteria for X.509 compliance is that the peer certificate must not contain less secure signature algorithms or Elliptic Curves (EC).

When you add or import the certificate, Secure Email and Web Manager performs X.509 validation of the certificate. Secure Email and Web Manager performs X.509 validation of the peer certificate if the X.509 validation is enabled during the peer certificate validation of the server. The detailed logging is tracked in the Secure Email and Web Manager system.current log files.

Related Topics

- [Validation of Peer Certificate, on page 556](#)
- [Custom CA Certificate Validation, on page 557](#)
- [Appliance Certificate Validation, on page 558](#)

Validation of Peer Certificate

AsyncOS provides a common configuration to control X.509 validation of the peer certificate for the following services under SSL configuration during TLS communication:

- Outbound SMTP
- LDAP
- Updater
- Alert over TLS
- Syslog Server
- Smart Licensing Server
- Security Services Exchange Connector
- Security Services Exchange Server

However, you must manually enable the X.509 validation of the peer certificate for Outbound SMTP, LDAP, Updater, and Alert over TLS. The X.509 validation of the peer certificate for the Syslog Server, Smart Licensing Server, Security Services Exchange Connector, and Security Services Exchange Server is performed by default.

You can configure the X.509 validation of the peer certificate using the web interface or CLI.

Related Topics

- [Validation of Peer Certificate using GUI, on page 557](#)
- [Validation of Peer Certificate using CLI, on page 557](#)

Validation of Peer Certificate using GUI

-
- Step 1** Navigate to **System Administration > SSL Configuration**.
The SSL Configuration page is displayed.
- Step 2** Click **Edit Settings**.
- Step 3** Check the **Enable** checkbox listed with **Peer Certificate X509 Validation**.
- Step 4** Click **Submit** and commit your changes.
-

Validation of Peer Certificate using CLI

You can use the `sslconfig` command to validate the peer certificate.

```
mail.example.com> sslconfig
```

```
Disabling SSLv3 is recommended for best security.
```

```
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.
```

```
Choose the operation you want to perform:
```

- VERSIONS - Enable or disable SSL/TLS versions
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, updater and LDAP.
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, updater and LDAP.

Custom CA Certificate Validation

AsyncOS does not perform an X.509 validation when you import the custom CA certificate into the Secure Email and Web Manager.

-
- Step 1** Enter the `CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT` command in the CLI.

```
mail.example.com> CERTCONFIG > CERTAUTHORITY > CUSTOM > IMPORT
```

- Step 2** Enter the name of the file you want to import.

```
mail.example.com> Enter the name of the file on machine "appliance" to import:  
[]> filename.pem
```

The file is imported without any validation.

Appliance Certificate Validation

AsyncOS performs an X.509 validation when you import the appliance certificate into the Secure Email and Web Manager. You must manually enable the validation.

Step 1 Enter the `CERTCONFIG > CERTIFICATE > SETUP` command in the CLI.

```
mail.example.com> CERTCONFIG > CERTIFICATE > SETUP
```

Step 2 Enter **Y** if you want to use a certificate or key for receiving, delivery, HTTPS management access, and LDAP.

```
Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and LDAPS?
AsyncOS performs an X.509 validation on the imported appliance certificate.
```

Single Pane of Glass

The Single Pane of Glass (SPoG) feature enables you to access Cisco Secure Email and Web Manager details on a single primary Cisco Secure Email and Web Manager. You must ensure that you have multiple Cisco Secure Email and Web Manager units connected to a primary Cisco Secure Email and Web Manager unit. You can view information for example Monitoring, Tracking, Quarantine of the secondary Cisco Secure Email and Web Manager units on a primary unit. However, to perform this, you must enable the configuration using the command line interface of the primary Cisco Secure Email and Web Manager.

Before you begin

Make sure all the Secure Email and Web Manager devices have the same version.

To enable the drop-down and gather information in the primary Cisco Secure Email and Web Manager unit, you must use the **smaapplianceconfig** command.

Once you enable the configuration, you can view the details of the secondary Cisco Secure Email and Web Managers in the primary unit, see [SPoG Viewing details on primary Cisco Secure Email and Web Manager, on page 563](#)



Note When you enable or disable SPoG, the session of all the users concurrently logged into NGUI becomes invalid, and a new request to the server logs them out. The users must log in again.

Also, if a Secure Email and Web Manager is added to SPoG or deleted from SPoG, and you are currently logged into the NGUI of the same Secure Email and Web Manager, then you will be logged out due to a change in the flow of JWT validation.



Note The users' or authentication-related setup should be the same across all the connected SPoG setups.

For example, suppose you are trying to log in as an externally authenticated user on the primary Secure Email and Web Manager; the same external authentication settings should be available on the secondary Secure Email and Web Manager to access secondary Secure Email and Web Managers from the primary Secure Email and Web Manager.

Using the **smaapplianceconfig** command you can:

- [SPoG Add a Cisco Secure Email and Web Manager, on page 559](#)
- [SPoG Edit a Cisco Secure Email and Web Manager, on page 560](#)
- [SPoG Delete a Cisco Secure Email and Web Manager, on page 562](#)
- [SPoG Enable Services on a Cisco Secure Email and Web Manager, on page 562](#)
- [SPoG Viewing details on primary Cisco Secure Email and Web Manager, on page 563](#)

SPoG Add a Cisco Secure Email and Web Manager

The following example shows how you can add a Cisco Secure Email and Web Manager.

```
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> ADD
Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[]> vm21sma0062.cs21
Enter a name to identify this appliance
[]> SMA0062
File transfer access via SSH is required to transfer reporting data, message logs, and
quarantine safelist/blocklist data from appliances
Would you like to configure file transfer access for this appliance? [Y]>
Would you like to use a custom ssh port to connect to this appliance? [N]>
Enter the login credentials for an administrator or an operator account on the appliance.
This will be used to obtain an SSH key for file transfers.
Username:
[]> admin
Passphrase:
[]>
Appliance 10.10.3.62 added.
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
```

```

= =====
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> added vm21sma0062.cs21
Changes committed: Tue Apr 27 10:28:01 2021 GMT
vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled

```

SPoG Edit a Cisco Secure Email and Web Manager

The following example shows how you can edit a secondary Cisco Secure Email and Web Manager connection parameters.

```

vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> EDIT
Enter the name or number of the appliance you wish to edit.
[]> 3
Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[10.10.3.62]>
Enter a name to identify this appliance
[SMA0062]> Tracking_SMA0062
File transfer access via SSH is required to transfer reporting data, message logs, and
quarantine safelist/blocklist data from appliances
Would you like to configure file transfer access for this appliance? [Y]>
Would you like to use a custom ssh port to connect to this appliance? [N]>
Appliance 10.10.3.62 was edited
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled

```

```

2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 Tracking_SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> SERVICES
Enter the name or number of the appliance you wish to configure.
[]> 1
Services for appliance "SMA63" at address 10.10.3.63:
-----
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Would you like Email Reporting to be enabled on this appliance? [N]>
Would you like Email Tracking to be enabled on this appliance? [Y]>
Would you like Spam Quarantines to be enabled on this appliance? [Y]>
Services for appliance "SMA63" at address 10.10.3.63:
-----
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
3 10.10.3.62 Tracking_SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> services
Enter the name or number of the appliance you wish to configure.
[]> 3
Services for appliance "Tracking_SMA0062" at address 10.10.3.62:
-----
Email Reporting service: Enabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Would you like Email Reporting to be enabled on this appliance? [Y]> N
Would you like Email Tracking to be enabled on this appliance? [Y]>
Would you like Spam Quarantines to be enabled on this appliance? [Y]> N
Services for appliance "Tracking_SMA0062" at address 10.10.3.62:
-----
Email Reporting service: Disabled
Email Tracking service: Enabled
Spam Quarantines service: Disabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.62 Tracking_SMA0062 Yes Disabled Enabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled

```

```

Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> use vm21sma0062.cs21 for tracking
Changes committed: Tue Apr 27 10:32:32 2021 GMT

```

SPoG Delete a Cisco Secure Email and Web Manager

The following example shows how you can delete a Cisco Secure Email and Web Manager.

```

vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 Tracking_SMA0062 Yes Disabled Enabled Disabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> DELETE
Enter the name or number of the appliance you wish to delete.
[]> 3
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
2 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> deleting Tracking_SMA0062
Changes committed: Tue Apr 27 10:37:12 2021 GMT
vm21sma0061.cs21>

```

SPoG Enable Services on a Cisco Secure Email and Web Manager

The following example shows how you can enable services on a Cisco Secure Email and Web Manager.

```

vm21sma0061.cs21> smaapplianceconfig
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====

```



```

1 10.10.3.62 SMA0062 Yes Disabled Disabled Disabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]> SERVICES
Enter the name or number of the appliance you wish to configure.
[]> 1
Services for appliance "SMA0062" at address 10.10.3.62:
-----
Email Reporting service: Disabled
Email Tracking service: Disabled
Spam Quarantines service: Disabled
Would you like Email Reporting to be enabled on this appliance? [N]> Y
Would you like Email Tracking to be enabled on this appliance? [N]> Y
Would you like Spam Quarantines to be enabled on this appliance? [N]> Y
Services for appliance "SMA0062" at address 10.10.3.62:
-----
Email Reporting service: Enabled
Email Tracking service: Enabled
Spam Quarantines service: Enabled
Enter the name or number of the appliance you wish to configure.
[]>
Security Appliances:
Management
# IP Name Authenticated Email Email Spam
Reporting Tracking Quarantines
= =====
1 10.10.3.63 SMA63 Yes Disabled Enabled Enabled
2 10.10.3.165 SMA165 Yes Enabled Enabled Disabled
3 10.10.3.62 SMA0062 Yes Enabled Enabled Enabled
Choose the operation you want to perform:
- ADD - Add a new appliance.
- EDIT - Edit an appliance.
- DELETE - Remove an appliance.
- SERVICES - Configure the centralized services for an appliance.
[]>
vm21sma0061.cs21> commit
Please enter some comments describing your changes:
[]> anabled services on vm21sma0062.cs21
Changes committed: Tue Apr 27 10:29:17 2021 GMT
vm21sma0061.cs21>

```

SPoG Viewing details on primary Cisco Secure Email and Web Manager

To view the details of the secondary units, you must:

- Navigate to the Quarantine page of the primary Cisco Secure Email and Web Manager unit.
- Select the secondary Cisco Secure Email and Web Manager from the **View SMA** drop down.

You can now view the data corresponding to the selected secondary Cisco Secure Email and Web Manager on your primary unit.

You can also view the same in both the Tracking and Monitoring pages after you enable using the **services** sub command in the **smaapplianceconfig** command.



CHAPTER 18

Logging

This chapter contains the following sections:

- [Logging Overview](#), on page 565
- [Log Types](#), on page 569
- [Log Subscriptions](#), on page 591

Logging Overview

Log files record regular operations, as well as exceptions, for activity on the system. Use the logs for monitoring the Cisco Content Security appliance, troubleshooting, and evaluating system performance.

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 Cisco Content Security Management appliance.



Note The Security Management appliance pulls information for all reporting and tracking with the exception of spam quarantine data. This data is pushed from the ESA.

Log Retrieval

Log files can be retrieved with the file transfer protocols described in the following table. You set the protocol when you create or edit a log subscription in the GUI, or by using the `logconfig` command in the CLI.

FTP Poll	<p>With this type of file transfer, a remote FTP client accesses the appliance to retrieve log files by using the user name and passphrase 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.</p>
FTP Push	<p>With this type of file transfer, the appliance periodically pushes log files to an FTP server on a remote computer. The subscription requires a user name, passphrase, and destination directory on the remote computer. Log files are transferred based on the configured rollover schedule.</p>
SCP Push	<p>With this type of file transfer, the 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 SSH2 protocol. The subscription requires a user name, SSH key, and destination directory on the remote computer. Log files are transferred based on the configured rollover schedule.</p>
Syslog Push	<p>With this type of file transfer, the 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, by default. In AsyncOS 14.1.0, the port number ranges from 1-65535. 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.</p> <p>Enter maximum size of the log message to send to the remote server. [For TCP protocol] The maximum message size value must be an integer from 1024 to 65535 and [For UDP protocol] The maximum message size value must be an integer from 1024 to 9216</p> <p>Use the TLS option to send log messages from your Cisco Secure Email and Web Manager to the remote syslog server over a TLS connection.</p> <p>Note If you select the TLS option, make sure you add a valid client certificate in your Secure Email and Web Manager to establish a TLS connection between your Cisco Secure Email and Web Manager and the remote syslog server.</p>

Syslog Push	<p>Syslog Disk Buffer - [Applicable for TCP protocol only]: Select this check box to configure a local disk buffer for a syslog push log subscription to allow Secure Email and Web Manager to cache log events when the remote syslog server is unavailable. When the syslog server becomes available, the Secure Email and Web Manager begins to send all the data in the buffer for that log subscription to the syslog server.</p> <p>Note:</p> <ul style="list-style-type: none"> • Ensure that the syslog server is running before starting this procedure to avoid loss of log data. • Determine the size of the local disk buffer, allowing enough space to accommodate the maximum expected period of down time for the syslog server. This avoids the loss of log data. • If you have a secondary log subscription for local retention, Cisco recommends you cancel the secondary subscription to allow space for the local disk buffer for the primary subscription. • The Secure Email and Web Manager may not be able to cache the first several seconds of log data after loss of connection to the syslog server. This is due to characteristics of syslog over TCP. • The default syslog disk buffer size is 100MB. The maximum disk buffer size allowed is 1GB. You can enter the size in bytes (1073741824), megabytes(1M), or gigabytes(1G).
-------------	--

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

When you create a log subscription, you specify the trigger(s) for when the logs roll over, the old file is transferred, and a new log file is created.

Choose between the following triggers:

- File size
- Time

- At a specified interval (in seconds, minutes, hours, or days)

Follow the example on the screen when entering values.

To enter a composite interval, such as two-and-a-half hours, follow the example 2h30m .

or

- Every day, at the time(s) you specify

or

- On the days of the week that you select, at the time(s) you specify

When you specify times, use the 24-hour format, for example 23:00 for 11pm.

To schedule multiple rollover times in a day, separate times with a comma. For example, to roll over logs at midnight and noon, enter 00:00, 12:00

Use an asterisk (*) as a wildcard. For example, to roll over logs exactly at every hour and half-hour, enter *:00, *:30

When the specified limit is reached (or the first limit is reached, if you have configured both size- and time-based limits), 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 appliance until they are retrieved or until the system needs more space for log files.



Note If a rollover is in progress when the next limit is reached, the new rollover is skipped. An error will be logged and an alert sent.

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

Logs Enabled by Default

The Security Management appliance is preconfigured with the following log subscriptions enabled.

Table 88: Preconfigured Log Subscriptions

Log Name	Log Type	Retrieval Method
cli_logs	CLI audit logs	FTP Poll
euq_logs	Spam quarantine logs	FTP Poll
euqgui_logs	Spam quarantine GUI logs	FTP Poll

Log Name	Log Type	Retrieval Method
gui_logs	HTTP logs	FTP Poll
mail_logs	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, on page 592](#).

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, on page 591](#).

Log Types

- [Summary of Log Types, on page 569](#)
- [Using Configuration History Logs, on page 574](#)
- [Using CLI Audit Logs, on page 574](#)
- [Using FTP Server Logs, on page 575](#)
- [Using HTTP Logs, on page 576](#)
- [Using Spam Quarantine Logs, on page 576](#)
- [Using Spam Quarantine GUI Logs, on page 577](#)
- [Using Text Mail Logs, on page 577](#)
- [Using NTP Logs, on page 583](#)
- [Using Reporting Logs, on page 583](#)
- [Using Reporting Query Logs, on page 584](#)
- [Using Safelist/Blocklist Logs, on page 584](#)
- [Using SMA Logs, on page 585](#)
- [Using Status Logs, on page 586](#)
- [Using System Logs, on page 588](#)
- [Understanding Tracking Logs, on page 589](#)
- [Using Audit Logs, on page 589](#)

Summary of 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, on page 591](#) for more information.

AsyncOS generates the following log types:

Table 89: Log Types

Log Type	Description
Authentication Logs	The authentication log records successful logins and unsuccessful login attempts, for locally and externally authenticated users, for both GUI and CLI access to the Security Management appliance. In Debug and more verbose modes, if external authentication is turned on, all LDAP queries appear in these logs.
Backup Logs	Backup logs record the backup process from start to finish. Information about backup scheduling is in the SMA logs.
CLI Audit Logs	The CLI audit logs record all CLI activity on the system.
Configuration History Logs	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.
FTP Server Logs	FTP logs record information about the FTP services enabled on the interface. Connection details and user activity are recorded.
GUI logs	GUI logs include a history of page refreshes in the web interface, session data, and the pages a user accesses. You can use the <code>gui_log</code> to track user activity or investigate errors that users see in the GUI. The error traceback will normally be in this log. GUI logs also include information about SMTP transactions, for example information about scheduled reports emailed from the appliance.
HTTP Logs	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.
Haystack logs	Haystack logs record web transaction tracking data processing.
Text Mail Logs	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). For important information about when attachment names are included in mail logs, see Tracking Service Overview .

Log Type	Description
LDAP Debug Logs	<p>Use these logs to debug problems when you are configuring LDAP in System Administration > LDAP.</p> <p>For example, these logs record the results of clicking the Test Server and Test Queries buttons.</p> <p>For information about failed LDAP authentications, see the Authentication logs.</p>
NTP Logs	NTP logs record the conversation between the appliance and any configured Network Time Protocol (NTP) servers. For information about configuring NTP servers, see Configuring the System Time, on page 510 .
Reporting Logs	Reporting logs record actions associated with the processes of the centralized reporting service.
Reporting Query Logs	Reporting query logs record actions associated with the reporting queries that are run on the appliance.
SMA Logs	<p>SMA logs record actions associated with general Security Management appliance processes, not including the processes of the centralized reporting, centralized tracking, and spam quarantine services.</p> <p>These logs include information about backup scheduling.</p>
SNMP Logs	SNMP logs record debug messages related to the SNMP network management engine. In Trace or Debug mode, this includes SNMP requests to the Security Management appliance.
Safelist/Blocklist Logs	Safelist/blocklist logs record data about the safelist/blocklist settings and database.
Spam Quarantine GUI Logs	Spam quarantine GUI logs record actions associated with the spam quarantine GUI, such as quarantine configuration through the GUI, end user authentication, and end user actions (for example, releasing email).
Spam Quarantine Logs	Spam quarantine logs record actions associated with the spam quarantine processes.
Status Logs	Status logs record system statistics found in the CLI status commands, including status detail and dnsstatus . The period of recording is set using the setup subcommand in logconfig . Each counter or rate reported in status logs is the value since the last time the counter was reset.
System Logs	System logs record the following: boot information, DNS status information, and comments users typed using the commit command. System logs are useful for troubleshooting the state of the appliance.
Tracking Logs	Tracking logs record actions associated with the processes of the tracking service. Tracking logs are a subset of the mail logs.
Updater Logs	Information about service updates, such as time zone updates.
Upgrade Logs	Status information about upgrade download and installation.

Log Type	Description
Audit Logs	<p>The Audit logs record AAA (Authentication, Authorization, and Accounting) events.</p> <p>Some of the audit log details are as follows:</p> <ul style="list-style-type: none"> • User - Logon • User - Logon failed incorrect password • User - Logon failed unknown username • User - Logon failed account expired • User – Logoff • User - Lockout • User - Activated • User - Password change • User - Password reset • User - Security settings/profile change • User - Created • User - Deleted or modified • User Configuration - Configuration changes made by the user. • Group/Role - Deletion or modified • Group /Role - Permissions change • Quarantine - Actions performed on messages in the quarantine.

Log Type Comparison

The following table summarizes the characteristics of each log type.

Table 90: Log Type Comparison

						Contains					
	Transa ctional	State less	Record ed as Text	Record ed as Binary	Header Logging	Periodic Status Informa tion	Message Receiving Informa tion	Delivery Informa tion	Indivi dual Hard Bounces	Indivi dual Soft Bounces	Configu ration Informa tion
Authenti cation Logs	•		•								
Backup Logs	•		•								

						Contains					
CLI Audit Logs	•		•			•					
Configuration History Logs	•		•								•
FTP Server Logs	•		•			•					
HTTP Logs	•		•			•					
Haystack Logs	•		•								
Text Mail Logs	•		•		•	•	•	•	•	•	
LDAP Debug Logs	•		•								
NTP Logs	•		•			•					
Reporting Logs	•		•			•					
Reporting Query Logs	•		•			•					
SMA Logs	•		•			•					
SNMP Logs	•		•								
Safelist/Blocklist Logs	•		•			•					
Spam Quarantine GUI	•		•			•					
Spam Quarantine	•		•			•					

						Contains					
Status Logs		•	•			•					
System Logs	•		•			•					
Tracking Logs	•			•	•		•	•	•	•	
Updater Logs	•		•								
Audit Logs			•								

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.

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: 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 "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

The following table describes the statistics recorded in CLI audit logs.

Table 91: 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.

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
=====
admin    Wed 11AM   3m 45s   10.1.3.14   tail\nadmin   02:32PM   0s       10.1.3.14
cli\nmail3.example.com> '
Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n- NEW
- Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

Using FTP Server Logs

The following table describes the statistics recorded in FTP server logs.

Table 92: 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).

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

The following table describes the statistics recorded in HTTP logs

Table 93: Statistics Recorded in HTTP Logs

Statistic	Description
Timestamp	Time that the bytes were transmitted.
ID	Session ID.
req	IP address of machine connecting.
user	User name of user connecting.
Message	Information regarding the actions performed. May include GET or POST commands or system status, and so forth.

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=recipientsin&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 Spam Quarantine Logs

The following table describes the statistics recorded in spam quarantine logs.

Table 94: 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).

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 Spam Quarantine GUI Logs

The following table shows the statistics recorded in spam quarantine GUI logs.

Table 95: 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.

Example

In this example, the log shows a successful authentication, login, and logout:

Table 96: 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 Text Mail Logs

These logs contain details of email receiving, email delivery, and bounces. These logs are a useful source of information to understand delivery of specific messages and to analyze system performance.

These logs do not require any special configuration. However, you must configure the system properly to view attachment names, and attachment names may not always be logged. For specifics, see [Tracking Service Overview](#).

The following table shows the information displayed in text mail logs.

Table 97: Text Mail Log Statistics

Statistic	Description
ICID	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.
DCID	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.
RCID	RPC Connection ID. This is a numerical identifier for an individual RPC connection to the spam quarantine. It is used to track messages as they are sent to and from the spam quarantine.
MID	Message ID. Use this to track messages as they flow through the logs.
RID	Recipient ID. Each message recipient is assigned an ID.
New	New connection initiated.
Start	New message started.

Sample Text Mail Log

Use the following sample as a guide to interpret log files.



Note Individual lines in log files are *not* numbered. They are numbered here only for sample purposes.

Table 98: Text Mail Log Detail

1	Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes
2	Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
3	Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>
4	Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>
5	Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>

6	Mon Apr 17 19:59:59 2003 Info: ICID 5 close
7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

The following table can be used as a guide to reading the previous log file.

Table 99: Detail of Text Mail Log Example

Line Number	Description
1	A new connection is initiated into the system and assigned an Injection ID (ICID) of "5." The connection was received on the Management IP interface and was initiated from the remote host at 10.1.1.209.
2	The message is assigned a Message ID (MID) of "6" after the MAIL FROM command is issued from the client.
3	The sender address is identified and accepted.
4	The recipient is identified and assigned a Recipient ID (RID) of "0."
5	MID 5 is accepted, written to disk, and acknowledged.
6	Receiving is successful and the receiving connection closes.
7	The message delivery process starts. It is assigned a Delivery Connection ID (DCID) of "8" from 192.168.42.42 and to 10.5.3.25.
8	The message delivery starts to RID "0."
9	Delivery is successful for MID 6 to RID "0."
10	The delivery connection closes.

Examples of Text Mail Log Entries

The following examples show log entries based on various cases.

Message Receiving

A message is injected into the 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)
```

Successful Message Delivery Example

```

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 appliance. Upon delivery, the destination host returns a 5XX error, which indicates that the message cannot be delivered to either recipient. The 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 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.

Successful Vault Health Check and Initialization

In this example, the log entry indicates that the vault health check and vault initialization are successful.

```
Tue Apr 2 06:12:48 2024 Info: The vault health check has passed, and the initialization
status is True.
```

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 antisipam
```

```
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 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 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: <stevell@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pemailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local 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

The following table shows the statistics recorded in NTP logs.

Table 100: 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.

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

The following table shows the statistics recorded in reporting logs.

Table 101: 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.

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

The following table shows the statistics recorded in reporting query logs.

Table 102: 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.

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_RECIP
IENTS_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

The following table shows the statistics recorded in safelist/blocklist logs.

Table 103: 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.

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: XXXXXXXXXXX-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

The following table shows the statistics recorded in SMA logs.

Table 104: 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.

Example

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.

Table 105: Status Log Statistics

Statistic	Description
CPULd	CPU utilization.
DskIO	Disk I/O utilization.
RAMUtil	RAM utilization.
QKUsd	Queue kilobytes used.
QKFre	Queue kilobytes free.
CrtMID	Message ID (MID).
CrtICID	Injection connection ID (ICID).
CRTDCID	Delivery connection ID (DCID).
InjMsg	Injected messages.
InjRcp	Injected recipients.
GenBncRcp	Generated bounce recipients.
RejRcp	Rejected recipients.
DrpMsg	Dropped messages.
SftBncEvt	Soft bounced events.
CmpRcp	Completed recipients.
HrdBncRcp	Hard bounced recipients.
DnsHrdBnc	DNS hard bounces.
5XXHrdBnc	5XX hard bounces.
FltrHrdBnc	Filter hard bounces.
ExpHrdBnc	Expired hard bounces.
OtrHrdBnc	Other hard bounces.
DlvRcp	Delivered recipients.

Statistic	Description
DelRep	Deleted recipients.
GlbUnsbHt	Global unsubscribe hits.
ActvRcp	Active recipients.
UnatmptRcp	Unattempted recipients.
AtmptRcp	Attempted recipients.
CrtCncIn	Current inbound connections.
CrtCncOut	Current outbound connections.
DnsReq	DNS requests.
NetReq	Network requests.
CchHit	Cache hits.
CchMis	Cache misses.
CchEct	Cache exceptions.
CchExp	Cache expired.
CPUTTm	Total CPU time used by the application.
CPUETm	Elapsed time since the application started.
MaxIO	Maximum disk I/O operations per second for the mail process.
RamUsd	Allocated memory in bytes.
SwIn	Memory swapped in.
SwOut	Memory swapped out.
SwPgIn	Memory paged in.
SwPgOut	Memory paged out.
MMLen	Total number of messages in the system.
DstInMem	Number of destination objects in memory.
ResCon	Resource conservation tarpit value. Acceptance of incoming mail is delayed by this number of seconds due to heavy system load.
WorkQ	Number of messages currently in the work queue.
QuarMsgs	Number of individual messages in the system quarantine (messages present in multiple quarantines are counted only once).
QuarQKUsd	Kilobytes used by system quarantine messages.

Statistic	Description
LogUsd	Percent of log partition used.
CASELd	Percent CPU used by CASE scanning.
TotalLd	Total CPU consumption.
LogAvail	Amount of disk space available for log files.
EuQ	Number of messages in the spam quarantine.
EuQRls	Number of messages in the spam quarantine release queue.

Example

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318
  DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15 FltrHrdBnc
0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp
  0 CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct
15395 CchExp 55085 CPUTTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen 0 DstInMem 4
ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3 TotalLd 3 LogAvail
17G EuQ 0 EuQRls 0
```

Using System Logs

The following table shows the statistics recorded in system logs.

Table 106: System Log Statistics

Statistic	Description
Timestamp	Time that the bytes were transmitted.
Message	The logged event.

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:Passphrase
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. The conversion tools are located at the following URL: <http://tinyurl.com/3c5l8r>.

Using Audit Logs

The Audit logs record AAA (Authentication, Authorization, and Accounting) events. Most information is at the debug or trace level.

Example of Audit Log Entries:

- In this example, the log shows when a user (for example, admin):
 - Logged in to the web interface of the appliance.
 - Logged out of the web interface of the appliance.

```
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Event: Successful login
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session established
successfully
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: User logged out
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session terminated
```

- In this example, the log shows that a user (for example, admin) entered the `logconfig` CLI command.


```
Thu Oct 8 13:33:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User input was 'logconfig'
Thu Oct 8 13:33:46 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User input was 'Enter'
```
- In this example, the log shows that a user (for example, admin) viewed the GUI pages on the legacy web interface of the appliance.


```
Thu Oct 8 13:35:07 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /network/dns, Event: User visited the web page.
```
- In this example, the log shows that a new user (for example, admin) is added to the appliance using the web interface, but the changes are not committed.

```
Thu Oct 8 13:36:30 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Added
user "admin" and changes
```

```
will reflect after commit.
Thu Oct 8 13:37:22 2020 Info: Appliance: maill.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Deleted
user "admin" and changes
will reflect after commit.
```

- In this example, the log shows that a user (for example, admin) discarded all the changes that were not committed on the web interface of the appliance.

```
Thu Oct 8 13:39:44 2020 Info: Appliance: maill.example.com, Interaction Mode: GUI,
User: admin,
Source IP: 192.168.1.1, Location: /commit, Event: User discarded all uncommitted changes.
```

- In this example, the log shows that a user (for example, admin) discarded all the changes that were not committed through the CLI.

```
Thu Oct 8 13:41:38 2020 Info: Appliance: maill.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: User discarded all uncommitted changes.
```

- In this example, the log shows that a user (for example, admin) made configuration changes to the Web UI session timeout.



Note You can view more details of the configuration changes made in your appliance by viewing the Configuration History Logs or by enabling the debug mode for the audit logs.

```
Thu Oct 8 13:45:46 2020 Info: Appliance: maill.example.com, User: admin,
Event: The following configuration changes were committed with comment - 'N/A'
Thu Oct 8 13:45:46 2020 Info: * [standalone] Number of seconds before the Web UI session
times out.
```

- In this example, the log shows that the AsyncOS APIs could not fetch the log subscriptions because the authentication failed.

```
Thu Oct 8 13:52:28 2020 Debug: 08/Oct/2020 13:52:28 +0000 Error - Code: 401,
Details: Unauthorized (No permission -- see authorization schemes)
Thu Oct 8 13:52:28 2020 Info: Appliance: maill.example.com, Interaction Mode: API,
User: admin, Role: Role Not Available, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Location: GET /sma/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: User is not
valid.
```

- In this example, the log shows that the AsyncOS APIs could fetch the log subscriptions because the authentication was successful.

```
Thu Oct 8 13:52:37 2020 Info: Appliance: maill.example.com, Interaction Mode: API,
User: admin, Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET /sma/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: API Access
Success.
```

- In this example, the log shows that:
 - A new user (for example, admin) is added to the appliance using the CLI, but the changes were not committed.
 - The existing user account details are updated in the appliance using the CLI, but the changes were not committed.

```
Thu Oct 8 13:42:48 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin, Source IP: 192.168.1.1, Event: Added user "hops" and changes will
reflect
after commit
Thu Oct 8 13:43:26 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
User: admin,
Source IP: 192.168.1.1, Event: Updated user "hops" and changes will reflect after
commit
```

- In this example, the log shows that a user (for example, admin) performed a message tracking search on the new web interface of the appliance.

```
User: admin,
Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET /sma/api/v2.0/message-tracking/messages?startDate=2020-10-12T00:00:00.000Z
&endDate=2020-10-12T04:13:00.000Z&ciscoHost=All_Hosts&searchOption=messages&offset=0&limit=100
HTTP/1.0,
Event: API Access Success.
```



Note The actions that you perform on the new web interface of the appliance (for example, tracking, reporting, or quarantine search) are recorded as logs based on the corresponding APIs used for these actions.

Log Subscriptions

- [Configuring Log Subscriptions, on page 591](#)
- [Creating a Log Subscription in the GUI, on page 593](#)
- [Configuring Global Settings for Logging, on page 594](#)
- [Rolling Over Log Subscriptions , on page 595](#)
- [Configuring Host Keys, on page 597](#)

Configuring Log Subscriptions

Log subscriptions create the individual log files that are stored on a Cisco Content Security 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 107: Log File Attributes

Attribute	Description
Log Type	Defines the type of information recorded and the format of the log subscription. For more information, see Summary of Log Types, on page 569 .
Name	Descriptive name of log subscription that you provide for your future reference.
Log Filename	Physical name of the file when it is written to disk. If the system includes multiple content security appliances, use a unique log filename to identify the appliance that generated the log file.

Attribute	Description
Rollover by File Size	Maximum size that the file can reach before it rolls over.
Rollover by Time	When to roll over log files, based on time. See options at Log Rollover and Transfer Schedule, on page 567 .
Rate Limit	Sets the maximum number of logged events in the log file, within the specified time range (in seconds). The default time range value is 10 seconds.
Log Level	Level of detail for each log subscription.
Retrieval Method	Method used to transfer the log files from the appliance.

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 [Summary of Log Types, on page 569](#). 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 passphrases. On the **Management Appliance > System Administration > Log Subscriptions** page, select `Yes` when prompted whether you want to include passphrase 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 108: Log Levels

Log Level	Description
Critical	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.
Warning	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.

Log Level	Description
Information	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.
Debug	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.
Trace	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

-
- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** On the **Management Appliance > System Administration > Log Subscriptions** page, click **Add Log Subscription**.
- Step 3** Select a log type and enter the log name (for the log directory), as well as the name for the log file itself.
- Step 4** If applicable, specify the maximum file size.
- Step 5** If applicable, specify days, times of day, or time intervals to roll over the logs. For more information, see [Log Rollover and Transfer Schedule, on page 567](#).
- Step 6** If applicable, specify the maximum number of logged events in the log file, within the specified time range (in seconds).
- Step 7** If applicable, specify the log level.
- Step 8** (Configuration history logs only) Select whether to include passphrases in the log.
- Note** You cannot load configurations containing masked passphrases. If you anticipate loading configurations from the configuration history logs, select Yes to include passphrases in the log.
- Step 9** Configure the log retrieval method.
- Step 10** Submit and commit your changes.
-

Editing Log Subscriptions

-
- Step 1** Click the name of the log in the Log Name column on the Log Subscriptions page.
- 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 Content Security appliance 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 Content Security 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 Content Security 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 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 109: Log Headers

Header name	Name of the header
Value	Contents of the logged header

For example, specifying “date, x-subject” as headers to be logged 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

- Step 1** Click the **Edit Settings** button in the Global Settings section of the Log Subscriptions page.
- 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.
For information about these settings, see [Configuring Global Settings for Logging, on page 594](#).
- Step 3** Enter any other headers you want to include in the logs. Separate each entry with a comma.
- Step 4** Submit and commit your changes.

Rolling Over Log Subscriptions

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)

What To Do Next

Rolling Over Logs in Log Subscriptions

See [Log Rollover and Transfer Schedule](#), on page 567.

Rolling Over Logs Immediately Using the GUI

-
- 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.
- Step 3** Click the **Rollover Now** button.
-

What to do next

- [Rolling Over Logs in Log Subscriptions](#) , on page 596
- [Rolling Over Logs Immediately via the CLI](#), on page 596

Rolling Over Logs Immediately 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 passphrase. 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.

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 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: "Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "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. "slbld_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 Content Security 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 user guide or online help for your Email Security appliance.

The `hostkeyconfig` subcommand performs the following functions:

Table 110: Managing Host Keys - List of Subcommands

Command	Description
New	Add a new key.
Edit	Modify an existing key.
Delete	Delete an existing key.
Scan	Automatically download a host key.
Print	Display a key.

Command	Description
Host	Display system host keys. This is the value to place in the remote system's "known_hosts" file.
Fingerprint	Display system host key fingerprints.
User	Display the public key of the system account that pushes the logs to the remote machine. This is the same key that appears when setting up an SCP push subscription. This is the value to place in the remote system's "authorized_keys" file.

Example - Scanning for Host Keys

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. SSH2:rsa
2. SSH2:dsa
3. All
[3]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed
]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed
]
Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed
]
2. mail3.example.com ssh-rsa [ key displayed
]
```

```
3. mail3.example.com 1024 35 [ key displayed
]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.

[]>
Currently configured logs:
[ list of configured logs
]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
mail3.example.com> commit
```




CHAPTER 19

Troubleshooting

This chapter contains the following sections:

- [Collecting System Information](#) , on page 601
- [Troubleshooting Hardware Issues](#) , on page 601
- [Troubleshooting Feature Setup Issues](#) , on page 601
- [General Troubleshooting Resources](#) , on page 602
- [Troubleshooting Issues with Specific Functionality](#) , on page 602
- [Working with Technical Support](#), on page 603
- [Running a Packet Capture](#), on page 606
- [Remotely Resetting Appliance Power](#) , on page 607

Collecting System Information

You can get information about your appliance and its status, including your serial number. Refer [Monitoring System Status](#), on page 363

Troubleshooting Hardware Issues

Lights on the front and/or rear panels of your hardware appliance indicate health and status of your appliance. For descriptions of these indicators, see the hardware guides such as the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide* available from the location specified in.

Specifications for your appliance, such as temperature ranges, are also available in these documents.



Note If you need to cycle power to your x80 or x90 appliance, wait at least 20 minutes for the appliance to come up (all LEDs are green) before pushing the power button.

Troubleshooting Feature Setup Issues

If you are experiencing difficulty configuring a feature successfully, see the summaries of the tasks you must complete for each feature. These include links to specific information for each.

- [Setting Up Centralized Web Reporting and Tracking](#) , on page 165
- [Setting Up Centralized Email Reporting](#), on page 50
- [Setting Up Centralized Message Tracking](#) , on page 250
- [Setting Up the Centralized Spam Quarantine](#)
- [Centralized Policy, Virus, and Outbreak Quarantines](#), on page 303
- [Using Configuration Masters to Centrally Manage Web Security Appliances](#) , on page 332

General Troubleshooting Resources

General troubleshooting resources include:

- Recent alerts. See [Viewing Recent Alerts](#) , on page 501.
- Log files. See [Logging](#), on page 565
- The Release Notes, including the Documentation Updates section. See [Documentation](#) , on page 629.
- The Cisco Bug Search Tool (instructions for access are in the Release Notes)
- [Knowledge Base Articles \(TechNotes\)](#) , on page 631
- [The Cisco Support Community](#), on page 631

Troubleshooting Issues with Specific Functionality

See also [Troubleshooting Feature Setup Issues](#) , on page 601.

Web Security-Related Issues

- [Troubleshooting All Reports](#) , on page 33
- [Troubleshooting Web Reporting and Tracking](#) , on page 241
- [Troubleshooting Configuration Management Issues](#) , on page 360
- Feature-related issues may also result from settings on your Web Security appliances. See the release notes and online help or user guide for your release at the location specified in [Documentation](#) , on page 629.

Email Security-Related Issues

- [Troubleshooting All Reports](#) , on page 33
- [Troubleshooting Message Tracking](#), on page 264
- [Troubleshooting Spam Quarantine Features](#) , on page 302
- [Troubleshooting Centralized Policy Quarantines](#) , on page 329
- Feature-related issues may also result from settings on your Email Security appliances. See the release notes and online help or user guide for your release at the location specified in [Documentation](#) , on page 629.

General Issues

- If you are unable to load a configuration file, make sure your disk space quotas are larger than the current size of each function in the table on the **Management Appliance > System Administration > Disk Management** page.
- If you have recently upgraded and the online help appears to be outdated or you cannot find the information about a new feature, clear your browser cache and then reopen the browser window.
- Unexpected behavior can occur when configuring settings using the web interface if you are using multiple browser windows or tabs simultaneously.
- See [Responding to Alerts](#) , on page 603.
- See [Troubleshooting Administrative User Access](#) , on page 433.

Responding to Alerts

- [Alert: Battery Relearn Timed Out \(RAID Event\) on 380 or 680 Hardware](#), on page 603
- [Additional Alert Descriptions](#) , on page 603

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

Problem: You receive an alert with subject “Battery Relearn Timed Out” for 380 or 680 hardware.

Solution: This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-related alerts from the system, then you can safely ignore this alert.

Additional Alert Descriptions

For descriptions of additional alerts, see

- [Hardware Alert Descriptions](#) , on page 502
- [System Alert Descriptions](#) , on page 502

What to do next

- [Managing Alerts](#), on page 499

Working with Technical Support

- [Opening or Updating a Support Case from the Appliance](#) , on page 603
- [Getting Support for Virtual Appliances](#) , on page 604
- [Enabling Remote Access for Cisco Technical Support Personnel](#) , on page 604

Opening or Updating a Support Case from the Appliance

You can use this method to contact Cisco TAC or your own support services.

Before you begin

If you wish to contact Cisco TAC:

- If your issue is urgent, do not use this method. Instead, contact support using one of the other methods listed in [Customer Support](#) , on page 632.
- Consider other options for getting help:
- When you open a support case using this procedure, the appliance configuration file is sent to Cisco Customer Support. If you do not want to send the appliance configuration, you can contact Customer Support using a different method.
- The appliance must be connected to the internet and able to send email.
- If you are sending information about an existing case, make sure you have the case number.

- Step 1** Log in to the appliance.
- Step 2** Choose **Help and Support > Contact Technical Support**.
- Step 3** Determine the recipients of the support request:

To send the request to Cisco TAC	Select the Cisco Technical Support check box.
To send the request only to your internal support desk	<ul style="list-style-type: none"> • Deselect the Cisco Technical Support check box. • Enter the email address of your support desk.
(Optional) To include other recipients	Enter email addresses.

- Step 4** Complete the form.
- Step 5** Click **Send**.

Getting Support for Virtual Appliances

If you file a support case for a Cisco content security virtual appliance, you must provide your Virtual License Number (VLN), your contract number, and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual appliance, by referencing your purchase order, or from the following table:

Functionality	PID	Description
All centralized web security functionality	SMA-WMGT-LIC=	—
All centralized email security functionality	SMA-EMGT-LIC=	

Enabling Remote Access for Cisco Technical Support Personnel

Only Cisco Customer Assistance can access your appliance using these methods.

- [Enabling Remote Access for Cisco Technical Support Personnel](#) , on page 604
- [Enabling Remote Access to Appliances Without a Direct Internet Connection](#) , on page 605

- [Disabling a Tech Support Tunnel , on page 606](#)
- [Disabling Remote Access , on page 606](#)
- [Checking the Status of the Support Connection , on page 606](#)

Enabling Remote Access to Appliances With an Internet Connection

Support accesses the appliance through an SSH tunnel that this procedure creates between the appliance and the upgrades.ironport.com server.

Before you begin

Identify a port that can be reached from the internet. The default is port25 which will work in most environment . Connections over this port are allowed in most firewall configurations.

-
- Step 1** Log in to the appliance.
 - Step 2** From the top right side of the GUI window, choose **Help and Support > Remote Access**.
 - Step 3** Click **Enable**.
 - Step 4** Enter information.
 - Step 5** Click **Submit**.
-

What to do next

When remote access for support personnel is no longer required, see [Disabling a Tech Support Tunnel , on page 606](#).

Enabling Remote Access to Appliances Without a Direct Internet Connection

For appliances without a direct internet connection, access is made through a second appliance that is connected to the internet.

Before you begin

- The appliance must be able to connect on port 22 to a second appliance that is connected to the internet.
- On the appliance with the internet connection, follow the procedure in [Enabling Remote Access to Appliances With an Internet Connection , on page 605](#) to create a support tunnel to that appliance.

-
- Step 1** From the command-line interface of the appliance requiring support, enter the `techsupport` command.
 - Step 2** Enter `sshaccess` .
 - Step 3** Follow the prompts.
-

What to do next

When remote access for support personnel is no longer required, see the following:

- [Disabling Remote Access , on page 606](#)
- [Disabling a Tech Support Tunnel , on page 606](#)

Disabling a Tech Support Tunnel

An enabled techsupport tunnel remains connected to upgrades.ironport.com for 7 days. After that time, established connections will not be disconnected but will be unable to re-attach to the tunnel once disconnected.

-
- Step 1** Log in to the appliance.
- Step 2** From the top right side of the GUI window, choose **Help and Support > Remote Access**.
- Step 3** Click **Disable**.
-

Disabling Remote Access

A remote access account that you create using the techsupport command remains active until you deactivate it.

-
- Step 1** From the command-line interface, enter the `techsupport` command.
- Step 2** Enter `sshaccess .`
- Step 3** Enter `disable .`
-

Checking the Status of the Support Connection

-
- Step 1** From the command-line interface, enter the `techsupport` command.
- Step 2** Enter `status .`
-

Running a Packet Capture

Packet Capture allows support personnel to see the TCP/IP data and other packets going into and out of the appliance. This allows Support to debug the network setup and to discover what network traffic is reaching the appliance or leaving the appliance.

-
- Step 1** Choose **Help and Support > Packet Capture**.
- Step 2** Specify packet capture settings:
- In the **Packet Capture Settings** section, click **Edit Settings**.
 - (Optional) Enter duration, limits, and filters for the packet capture.
- Your Support representative may give you guidance on these settings.
- If you enter a capture duration without specifying a unit of time, AsyncOS uses seconds by default.
- In the Filters section:
- Custom filters can use any syntax supported by the Unix `tcpdump` command, such as `host 10.10.10.10 && port 80 .`
-

- The client IP is the IP address of the machine connecting to the appliance, such as a mail client sending messages through the Email Security appliance.
- The server IP is the IP address of the machine to which the appliance is connecting, such as an Exchange server to which the appliance is delivering messages.

You can use the client and server IP addresses to track traffic between a specific client and a specific server, with the Email Security appliance in the middle.

c) Click **Submit**.

Step 3 Click **Start Capture**.

- Only one capture may be running at a time.
- When a packet capture is running, the Packet Capture page shows the status of the capture in progress by showing the current statistics, such as file size and time elapsed.
- The GUI only displays packet captures started in the GUI, not from the CLI. Similarly, the CLI only displays the status of a current packet capture run started in the CLI.
- The packet capture file is split into ten parts. If the file reaches the maximum size limit before the packet capture ends, 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.
- A running capture started in the GUI is preserved between sessions. (A running capture started in the CLI stops when the session ends.)

Step 4 Allow the capture to run for the specified duration, or, if you have let the capture run indefinitely, manually stop the capture by clicking **Stop Capture**.

Step 5 Access the packet capture file:

- Click the file in the **Manage Packet Capture Files** list and click **Download File**.
- Use FTP or SCP to access the file in the captures subdirectory on the appliance.

What to do next

Make the file available to Support:

- If you allow remote access to your appliance, technicians can access the packet capture files using FTP or SCP. See [Enabling Remote Access for Cisco Technical Support Personnel](#), on page 604.
- Email the file to Support.

Remotely Resetting Appliance Power

If the appliance requires a hard reset, you can reboot the appliance chassis remotely using a third-party Intelligent Platform Management Interface (IPMI) tool.

Restrictions

- Remote power cycling is available only on certain hardware.
For specifics, see [Enabling Remote Power Cycling](#), on page 472.
- If you want to be able to use this feature, you must enable it in advance.
For details, see [Enabling Remote Power Cycling](#), on page 472.

- Only the following IPMI commands are supported:

`status, on, off, cycle, reset, diag, soft`

Issuing unsupported commands will produce an “insufficient privileges” error.

Before you begin

- Obtain and set up a utility that can manage devices using IPMI version 2.0.
- Understand how to use the supported IPMI commands. See the documentation for your IPMI tool.

Step 1 Use IPMI to issue a supported power-cycling command to the IP address assigned to the Remote Power Cycle port, which you configured earlier, along with the required credentials.

For example, from a UNIX-type machine with IPMI support, you might issue the command:

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

where `192.0.2.1` is the IP address assigned to the Remote Power Cycle port and `remoteresetuser` and `passphrase` are the credentials that you entered while enabling this feature.

Step 2 Wait at least eleven minutes for the appliance to reboot.



APPENDIX **A**

IP Interfaces and Accessing the Appliance

This chapter contains the following sections:

- [IP Interfaces and Accessing the Appliance, on page 609](#)
- [IP Interfaces, on page 609](#)

IP Interfaces and Accessing the Appliance

You can access any IP interface you create on a Cisco Content Security appliance through a variety of services. By default, the following services are either enabled or disabled on each interface:

Table 111: 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 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 user guide or online help for your Email Security appliance.

Configuring IP Interfaces

The Management Appliance > Network > IP Interfaces page (and interface config 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 112: 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.
Broadcast address	AsyncOS automatically calculates the default broadcast address from the IP address and the netmask.
Hostname	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.
Allowed services	FTP, SSH, Telnet, 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 spam quarantine.



Note If you have completed the System Setup Wizard as described in [Setup, Installation, and Basic Configuration, on page 7](#) and committed the changes, the Management interface should already be configured on the appliance.

Creating IP Interfaces Using the GUI

Step 1 [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.

- Step 2** Choose **Management Appliance > Network > IP Interfaces**.
- Step 3** Click **Add IP Interface**.
- Step 4** Enter a name for the interface.
- Step 5** Select an Ethernet port and enter an IP address.
- Step 6** Enter the netmask for the IP address.
- Step 7** Enter a hostname for the interface.
- Step 8** Select the check box next to each service you want to enable on this IP interface. Change the corresponding port if necessary.
- Step 9** Select whether to enable redirecting HTTP to HTTPS for appliance management on the interface.
- Step 10** If you are using the 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 spam quarantine, and whether to use the hostname as the URL or provide a custom URL.
- Step 11** Submit and commit your changes.

Accessing the Appliance via FTP



Caution

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.


- Step 1** [New Web Interface Only] On the Security Management appliance, click  to load the legacy web interface.
- Step 2** Choose **Management Appliance > Network > IP Interfaces** page (or the `interfaceconfig` command) to enable FTP access for the interface.
 - Note** Remember to commit your changes before moving on to the next step.
- Step 3** 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`
- Step 4** 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 the following table.

Table 113: Directories Available for Access

Directory Name	Description
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	<p>Created automatically for logging via the Management Appliance > System Administration > Log Subscriptions page or the logconfig and rollovernow commands. See the “Logging” chapter in the user guide or online help for your Email Security appliance for a detailed description of each log.</p> <p>See “Log File Type Comparison” in the “Logging” chapter for the differences among each log file type.</p>
/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"> • Virtual Gateway mappings (<code>altsrchost</code>) • Configuration data in XML format (<code>saveconfig</code>, <code>loadconfig</code>) • Host Access Table (HAT) page (<code>hostaccess</code>) • Recipient Access Table (RAT) page (<code>rcptaccess</code>) • SMTP Routes page (<code>smtproutes</code>) • Alias tables (<code>aliasconfig</code>) • Masquerading tables (<code>masquerade</code>) • Message filters (<code>filters</code>) • Global unsubscribe data (<code>unsubscribe</code>) • Test messages for the <code>trace</code> command
/MFM	<p>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.</p> <p>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.</p>
/periodic_reports	The directory where all archived reports configured on the system are stored.

Step 5 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 the table *Directories Available for Access*. 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 passphrase (`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 passphrase: (type the passphrase)
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 passphrase: (type the passphrase)
test.txt          100% |*****| 1007      00:00
```

You can use secure copy (`scp`) as an alternative to FTP to transfer files to and from the content security appliance.



Note Only users in the operators and administrators group can use secure copy (`scp`) to access the appliance. For more information, see [About Reverting to an Earlier Version of AsyncOS, on page 495](#).

Accessing via a Serial Connection

If you are connecting to the appliance via a serial connection, use the following information for the console port.

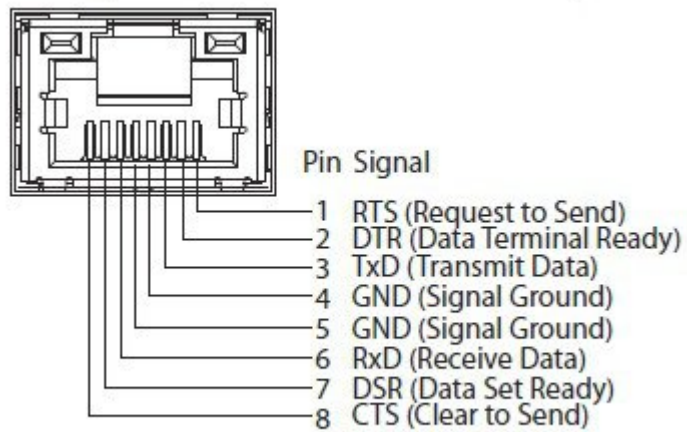
Complete information about this port is in the hardware installation guide for your appliance.

Related Topics

- [Documentation](#) , on page 629

Pinout Details for the Serial Port in 80- and 90- Series Hardware

Figure 21: Pinout Details for the Serial Port in 80- and 90- Series Hardware



Pinout Details for the Serial Port in 70-Series Hardware

The following figure illustrates the pin numbers for the serial port connector, and the table *Serial Port Pin Assignments* defines the pin assignments and interface signals for the serial port connector.

Figure 22: Pin Numbers for the Serial Port

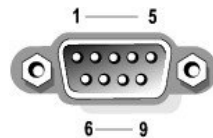


Table 114: Serial Port Pin Assignments

Pin	Signal	I/O	Definition
1	DCD		Data carrier detect
2	SIN		Serial input
3	SOUT		Serial output
4	DTR		Data terminal ready
5	GND	n/a	Signal ground
6	DSR		Data set ready
7	RTS		Request to send
8	CTS		Clear to send

Pin	Signal	I/O	Definition
9	RI		Ring indicator
Shell	n/a	n/a	Chassis ground



APPENDIX **B**

Assigning Network and IP Addresses

This appendix contains the following sections:

- [Ethernet Interfaces, on page 617](#)
- [Selecting IP Addresses and Netmasks, on page 617](#)
- [Strategies for Connecting Your Content Security Appliance , on page 619](#)

Ethernet Interfaces

Appliances have up to 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 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 appliance, these interface names can represent any two interfaces out of the three 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 content security 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 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 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 a appliance with the three network interfaces configured, each on a different network segment (assume all /24):

Ethernet	IP
Management	192.19.0.100
Data1	192.19.1.100

Ethernet	IP
Data2	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 content security appliance must always be able to identify a unique interface over which a packet can be delivered. To make this decision, the 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:

	Same Network	Different Network
Same Physical Interface	Allowed	Allowed
Different Physical Interface	Not allowed	Allowed

Strategies for Connecting Your Content Security Appliance

Keep the following in mind when connecting your 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 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

This chapter contains the following sections:

- [Firewall Information, on page 621](#)

Firewall Information

The following table lists the possible ports that may need to be opened for proper operation of Cisco Secure Email Gateway (these are the default values).

Table 115: Firewall Ports

Default Port	Protocol	In/Out	Hostname	Purpose
20/21	TCP	In or out	AsyncOS IPs, FTP server	FTP for aggregation of log files. Data ports TCP 1024 and higher must also all be open. For more information, search for FTP port information in the Knowledge Base. See Knowledge Base Articles (TechNotes) , on page 631 .
22	SSH	Out	AsyncOS IPs	Centralized configuration manager configuration push. Also used for backups.
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.
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.
80	HTTP	In	AsyncOS IPs	HTTP access to the GUI for system monitoring.
80	HTTP	Out	downloads.ironport.com	Service updates, except for AsyncOS upgrades .
80	HTTP	Out	upgrades.ironport.com	AsyncOS upgrades.
801	HTTP	In and Out	AsyncOS IPs	HTTP access to the GUI using <code>trailblazerconfig</code> CLI command.
82	HTTP	In	AsyncOS IPs	Used for viewing the spam quarantine.
83	HTTPS	In	AsyncOS IPs	Used for viewing the spam quarantine.
110	TCP	Out	POP server	POP authentication for end users for spam quarantine.
123	UDP	In & Out	NTP server	NTP if time servers are outside firewall.
143	TCP	Out	IMAP server	IMAP authentication for end users for spam quarantine.
161	UDP	In	AsyncOS IPs	SNMP Queries.
162	UDP	Out	Management station	SNMP Traps.
389 or 3268	LDAP	Out	LDAP servers	LDAP if LDAP directory servers are outside firewall. LDAP authentication for Cisco Spam Quarantine.
636 or 3269	LDAPS	Out	LDAPS	LDAPS — ActiveDirectory's global catalog server (uses SSL).
443	TCP	In	AsyncOS IPs	Secure HTTP (https) access to the GUI for system monitoring.
443	TCP	Out	update-static.ironport.com	Verify the latest files for the update server.

443	TCP	Out	update-manifests.ironport.com	Obtain the list of the latest files from the update server (for physical hardware email gateways.)
443	TCP	Out	update-manifests.sco.cisco.com	Obtain the list of the latest files from the update server (for virtual email gateways.)
443	TCP	Out	phonehome.senderbase.org	Receive/send Outbreak Filters.
443	TCP	Out	File Analysis server URL as configured on your Web Security appliance on the Security Services > Anti-Malware and Reputation page, in the Advanced section > Advanced Settings for File Analysis. File Analysis server URL as configured on your Email Security appliance on the Security Services > File Reputation and Analysis page, in the Advanced Settings for File Analysis section.	Display detailed file analysis results on the File Analysis server. <ul style="list-style-type: none"> • Web security reporting: (Cloud File Analysis) Ensure That the Management Appliance Can Reach the File Analysis Server , on page 183
443	HTTPS	In and Out	api-sse.cisco.com	Used to register your email gateway with Cisco Threat Response.
443	HTTPS	In and Out	api.eu.sse.itd.cisco.com	Used to register your email gateway with Cisco Threat Response.
443	HTTPS	In and Out	est.sco.cisco.com	Used to download a certificate to verify whether your email gateway is accessing a verified site when registering to Cisco Threat Response.
443	HTTPS	In and Out	AsyncOS IPs	HTTPS access to the GUI using <code>trailblazerconfig</code> CLI command.
514	UDP/TCP	Out	Syslog server	Syslog logging.
1024 and higher	—	—	—	See information above for Port 21 (FTP.)

7025	TCP	In and out	AsyncOS IPs	Pass policy, virus, and outbreak quarantine data between Cisco Secure Email Gateways and Cisco Secure Manager Email and Web Gateways when this feature is centralized.
32137	TCP			
6080	HTTP	In or Out		Access to API ports for HTTP Server
6443	HTTPS	In or Out		Access to API ports for HTTPS Server



APPENDIX **D**

Web Security Management Examples

This chapter contains the following sections:

- [Web Security Management Examples, on page 625](#)

Web Security Management Examples

This appendix illustrates and describes a number of common ways to implement features of the Cisco Content Security Management appliance, and includes the following sections:

- [Example 1: Investigating a User , on page 625](#)
- [Example 2: Tracking a URL, on page 627](#)
- [Example 3: Investigating Top URL Categories Visited, on page 627](#)

Web Security Appliance Examples

This section describes examples using a Security Management appliance and Web Security appliances.



Note All of these scenarios assume 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 [Using Centralized Web Reporting and Tracking, on page 163](#)

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**.

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.

Step 3 Click on IP address 10.251.60.24.

The User Details page appears for 10.251.60.24.

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. 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 Proxy Services tab on the Web Tracking page.

Step 5 Choose **Web > Reporting > Web Tracking**.

Step 6 Click the **Proxy Services** tab.

Step 7 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 search results appear.

From this page you can view a full list of transactions and URLs visited by the user of the computer that is assigned to the IP Address 10.251.60.24.

Related Topics

The following table lists each of the topics discussed in this example. Click on the link for details on each topic.

Table 116: Related Topics for Investigating a User

Feature Name	Feature Information
User Page	Users Report (Web) , on page 172
User Details Page	User Details (Web Reporting) , on page 173
Exporting Report Data	Exporting Reporting and Tracking Data , on page 31
Proxy Services tab on the Web Tracking page	Searching for Transactions Processed by Web Proxy Services , on page 229

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**.

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

The following table lists each of the topics discussed in this example. Click on the link for details on each topic.

Table 117: Related Topics for Tracking a URL

Feature Name	Feature Information
Web Sites Page	Web Sites Report , on page 175

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**.

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 NEEDS NEW ILLO - SKIP Scroll down to the **URL Categories Matched** table, to view the Bandwidth Used column.

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.

From this page, the network manager can see the top 10 users for Instant Messaging sites.

This page 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

The following table lists each of the topics discussed in this example. Click on the link for details on each topic.

Table 118: Related Topics for Investigating the Top URL Categories

Feature Name	Feature Information
URL Categories Page	URL Categories Report , on page 176
Exporting Report Data	Exporting Reporting and Tracking Data , on page 31



APPENDIX **E**

Additional Resources

This chapter contains the following sections:

- [Cisco Notification Service](#) , on page 629
- [Documentation](#) , on page 629
- [Third Party Contributors](#), on page 630
- [Training](#), on page 630
- [Knowledge Base Articles \(TechNotes\)](#) , on page 631
- [Registering Azure Active Directory Application](#), on page 631
- [Cisco Support Community](#), on page 631
- [Customer Support](#) , on page 632
- [Registering for a Cisco Account](#) , on page 632
- [Cisco Welcomes Your Comments](#), on page 632

Cisco Notification Service

Sign up to receive notifications relevant to your Cisco Content Security Appliances, such as Security Advisories, Field Notices, End of Sale and End of Support statements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit <http://www.cisco.com/cisco/support/notifications.html>

A Cisco.com account is required. If you do not have one, see [Registering for a Cisco Account](#) , on page 632.

Documentation

Documentation for this product and related products is available at the following locations:

Documentation For Cisco Content Security Products:	Is Located At:
Cisco Secure Email and Web Manager	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html Hardware and virtual appliance information: http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html MIBs: Monitoring System Health Using SNMP , on page 474
Secure Web Appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email Gateway	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Command Line Reference guide for content security products	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

You can also access the HTML online help version of the user guide directly from the appliance GUI by clicking **Help and Support** in the upper-right corner.

Third Party Contributors

Some software included within 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 license agreements.

Information about third-party licenses is available in a Licensing document at: <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html> and at https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

Portions of the software within 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.

Training

For training options, see:

- <http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html>

- <http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html>

Knowledge Base Articles (TechNotes)

Procedure

	Command or Action	Purpose
Step 1	Go to the main product page (http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html)	
Step 2	Look for links with TechNotes in the name.	

Registering Azure Active Directory Application

To register an Azure Active Directory application to access the identity information, perform the following steps:

-
- Step 1** Sign in to the <https://portal.azure.com/#home> portal.
 - Step 2** Use the **Directory + subscription** filter in the top menu to select the tenant in which you want to register an application if you have access to multiple tenants.
 - Step 3** Search and select **Azure Active Directory**.
 - Step 4** Select **App registrations > New registration** under **Manage**.
 - Step 5** Enter a **Name** for your application. The users of your application can see the name, and you can modify it later.
 - Step 6** Select the **Supported account types** for the application.
 - Step 7** Select **Web** in application type.
 - Step 8** Enter the redirect URL.
 - Step 9** Select **Register** to create the application registration.
-

Cisco Support Community

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

Access the Cisco Support Community at the following URLs:

- For email security and associated management:
<https://supportforums.cisco.com/community/5756/email-security>
- For web security and associated management:
<https://supportforums.cisco.com/community/5786/web-security>

Customer Support

Use the following methods to obtain support:

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support site for legacy IronPort: <http://www.cisco.com/web/services/acquisitions/ironport.html>

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

See also [Opening or Updating a Support Case from the Appliance](#) , on page 603.

For virtual appliances, see the *Cisco Content Security Virtual Appliance Installation Guide*.

Registering for a Cisco Account

Access to many resources on Cisco.com requires a Cisco account.

If you do not have a Cisco.com User ID, you can register for one here: <https://tools.cisco.com/RPF/register/register.do>

Related Topics

- [Cisco Notification Service](#) , on page 629
- [Knowledge Base Articles \(TechNotes\)](#) , on page 631

Cisco Welcomes Your Comments

The Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:

contentsecuritydocs@cisco.com

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



APPENDIX **F**

End User License Agreement

This chapter contains the following sections:

- [Cisco Systems End User License Agreement](#) , on page 633
- [Supplemental End User License Agreement for Cisco Systems Content Security Software](#) , on page 639

Cisco Systems End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER

PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE / SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1) THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

- (i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;
- (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;
- (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;
- (iv) publish any results of benchmark tests run on the Software;
- (v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or
- (vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. NOT WITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

<https://www.cisco.com/c/en/us/about/legal/global-export-trade/general-export/contract-compliance.html>.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms. The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on <https://www.cisco.com/>) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s)."

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual

development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING

IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and

warranties ("Warranties") are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

<https://www.cisco.com/c/en/us/products/warranty-listing.html>

Supplemental End User License Agreement for Cisco Systems Content Security Software

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

- Cisco AsyncOS for Email
- Cisco AsyncOS for Web
- Cisco AsyncOS for Management
- Cisco Email Anti-Spam, Sophos Anti-Virus
- Cisco Email Outbreak Filters
- Cloudmark Anti-Spam
- Cisco Image Analyzer
- McAfee Anti-Virus
- Cisco Intelligent Multi-Scan
- Cisco RSA Data Loss Prevention
- Cisco Email Encryption
- Cisco Email Delivery Mode
- Cisco Web Usage Controls
- Cisco Web Reputation
- Sophos Anti-Malware
- Webroot Anti-Malware
- McAfee Anti-Malware
- Cisco Email Reporting
- Cisco Email Message Tracking
- Cisco Email Centralized Quarantine
- Cisco Web Reporting
- Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk
Email Encryption for Encryption Appliances
Email Encryption for System Generated Bulk Email
Email Encryption and Public Key Encryption for Encryption Appliances
Large Attachment Handling for Encryption Appliances
Secure Mailbox License for Encryption Appliances

Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at <http://www.cisco.com/c/en/us/about/legal/service-descriptions.html>.

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

Consent and License to Use Data.

Subject to the Cisco Privacy Statement at <http://www.cisco.com/web/siteassets/legal/privacy.html>, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.



INDEX

A

alternate release appliance [311](#)
anti-virus quarantine. See quarantine, virus [304](#)

B

base entropy value, for password strength [416](#)

C

clean messageemail [64](#)
 clean message [64](#)
content filters [304](#)

D

data loss prevention [304](#)
delete all messages in the spam quarantine [301](#)
DNS [68](#), [507](#)
 authoritative server [507](#)
 double lookup [68](#)
 servers [507](#)
 splitting [507](#)
Domain-Based Executive Summary Report [149](#)
double-DNS verified [67](#), [125](#)

E

Early Expiration [312](#)
 for quarantine [312](#)
Email Security Appliance [52](#), [272](#)
 adding as managed appliance [52](#), [272](#)
End User Quarantine [289](#)
 see spam quarantine, end user access [289](#)

G

graymail [64](#)

I

IMAP authentication [290](#)
invalid recipient [64](#)

IronPort Spam Quarantine. See Spam quarantine [304](#)

L

LDAP [287](#), [289](#)

M

mailing lists [294](#)
 notifications [294](#)
marketing messages [64](#)
message filters [304](#)
message variables [292](#)
 spam quarantine notifications [292](#)
monitoring [49](#), [152](#)
 scheduling reports [152](#)
 summary data [49](#)

N

Normal Expiration [312](#)
 for quarantine [312](#)

P

passwords [416](#)
 requirements [416](#)
POP authentication [290](#)
PVO. See quarantines, policy, virus, and outbreak [304](#)

Q

quarantine [304](#), [312–313](#), [316](#), [322–323](#), [325](#), [329](#)
 applying actions to messages in [323](#)
 default action [313](#), [316](#)
 early expiration [312](#)
 In other quarantines [325](#)
 international character sets [322](#)
 normal expiration [312](#)
 outbreak [304](#)
 outbreak, reporting messages to Cisco [329](#)
 retention time [312](#)
 spam. See Spam quarantine [304](#)
 unclassified [316](#)

- quarantine (*continued*)
 - virus [304](#)
 - quarantine. See also Quarantines [311](#)
 - quarantines [304, 311](#)
 - policy [304](#)
 - policy, virus, and outbreak, centralized [311](#)
 - disabling [311](#)
 - policy, virus, and outbreak, managing [311](#)
 - types [304](#)
 - quarantines. See also Quarantine. [311](#)
- ## R
- reports [152](#)
 - scheduling [152](#)
 - time range [152](#)
 - for scheduled reports (email) [152](#)
 - Retention Time [312](#)
 - for quarantines [312](#)
- ## S
- safelist/blocklist [277–279, 285–286](#)
 - and external spam quarantine [279](#)
 - backing up and restoring [285](#)
 - enabling [278](#)
 - importing and exporting [285](#)
 - managing [279](#)
 - troubleshooting [286](#)
 - workqueue [277](#)
 - SenderBase [68](#)
 - spam message [64](#)
 - spam quarantine [267–268, 270, 287–289, 292, 294–295, 300–301](#)
 - alias consolidation [294](#)
 - behavior when full [268, 270](#)
 - deleting all messages [301](#)
 - disabling [301](#)
 - end user access [289](#)
 - end-user access [287](#)
 - external [267](#)
 - IMAP/POP authentication [289](#)
 - LDAP authentication [288](#)
 - local [267](#)
 - spam quarantine (*continued*)
 - message details [300](#)
 - message variables [292](#)
 - notification [292](#)
 - receiving multiple notifications [294](#)
 - released messages and email pipeline [301](#)
 - testing notifications [295](#)
 - stopped by content filter [60, 64](#)
 - stopped by reputation filtering [64](#)
 - System Capacity report [92–94, 106–108](#)
 - Email [92–94, 106–108](#)
 - All page [94, 108](#)
 - Incoming Mail page [93, 106](#)
 - memory page swapping [94, 107](#)
 - Outgoing Mail page [93, 107](#)
 - System Load page [93, 107](#)
 - WorkQueue page [92, 106](#)
 - system quarantine. See quarantines, policy, virus, and outbreak [304](#)
- ## T
- TLS Connections page [56](#)
- ## U
- unclassified quarantine. See quarantine, unclassified [304](#)
 - user accounts [414, 416, 420](#)
 - locking and unlocking [416, 420](#)
 - user groups [404](#)
 - user roles [404](#)
 - descriptions [404](#)
- ## V
- virus message [64](#)
 - virus quarantine. See quarantine [304](#)
 - virus. [304](#)
- ## W
- Web UI session timeout [429–430](#)