Logging

This chapter contains the following sections:

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	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.
FTP Push	With this type of file transfer, the Cisco Content Security 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.
SCP Push	With this type of file transfer, the Cisco Content Security 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.
Syslog Push	With this type of file transfer, the Cisco Content Security appliance sends log messages to a remote syslog server. This method conforms to RFC 3164. You must submit a hostname for the syslog server and use either UDP or TCP for log transmission. The port used is 514. A facility can be selected for the log; however, a default for the log type is preselected in the drop-down menu. Only text-based logs can be transferred using syslog push.

Filename and Directory Structure

AsyncOS creates a directory for each log subscription based on the log name specified in the log subscription. The filenames of logs in the directory consist of the filename specified in the log subscription, the timestamp when the log file was started, and a single-character status code. The following example shows the convention for the directory and filename:

/<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>

Status codes may be .c (signifying “current”) or .s (signifying “saved”). You should only transfer log files with the saved status.

Log Rollover and Transfer Schedule

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 1: Preconfigured Log Subscriptions

Log Name	Log Type	Retrieval Method
cli_logs	CLI audit logs	FTP Poll
euq_logs	Spam quarantine logs	FTP Poll

Log Name	Log Type	Retrieval Method
euqgui_logs	Spam quarantine GUI logs	FTP Poll
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 24.

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 23.

Log Types

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 23 for more information.

AsyncOS generates the following log types:

Table 2: 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 gui_log 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	Use these logs to debug problems when you are configuring LDAP in System Administration > LDAP. For example, these logs record the results of clicking the Test Server and Test Queries buttons. For information about failed LDAP authentications, see the Authentication logs.
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.
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	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. These logs include information about backup scheduling.
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 Comparison

The following tablesummarizes the characteristics of each log type.

Table 3: Log Type Comparison

						Contains					
	Transactional	Stateless	Recorded as Text	Recorded as Binary	Header Logging	Periodic Status Information	Message Receiving Information	Delivery Information	Individual Hard Bounces	Individual Soft Bounces	Configuration Information
Authentication Logs	•		•								
Backup Logs	•		•								
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	•		•			•					

						Contains					
SMA Logs	•		•			•					
SNMP Logs	•		•								
Safelist/ Blocklist Logs	•		•			•					
Spam Quarantine GUI	•		•			•					
Spam Quarantine	•		•			•					
Status Logs		•	•			•					
System Logs	•		•			•					
Tracking Logs	•			•	•		•	•	•	•	
Updater 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 4: 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
========  ==========  =========  ===========  ====\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 5: 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 tabledescribes the statistics recorded in HTTP logs

Table 6: 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 7: 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 8: 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 9: 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 10: 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 11: 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 12: 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."

Line Number	Description
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)
 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.

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 antispam
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: <stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
```

```
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make it
 a reality'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient policy
 DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local 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 13: 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 14: 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 15: 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_RECI
PIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
 None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from 0
to 2 sort_ascendin
g=False.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct  2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
 with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning results
 from 0 to 2 sort
_ascending=False.
Tue Oct  2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

Using Safelist/Blocklist Logs

The following table shows the statistics recorded in safelist/blocklist logs.

Table 16: 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: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC: 10800 seconds
Fri Sep 28 14:22:33 2007 Info: System is coming up.
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
.........................
Mon Oct  1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
Mon Oct  1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
Mon Oct  1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct  1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct  1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

Using SMA Logs

The following table shows the statistics recorded in SMA logs.

Table 17: 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 18: Status Log Statistics

Statistic	Description
CPULd	CPU utilization.
DskIO	Disk I/O utilization.
RAMUtil	RAM utilization.
QKUsd	Queue kilobytes used.
QKFre	Queue kilobytes free.
CrtMID	Message ID (MID).
CrtICID	Injection connection ID (ICID).
CRTDCID	Delivery connection ID (DCID).
InjMsg	Injected messages.
InjRcp	Injected recipients.
GenBncRcp	Generated bounce recipients.
RejRcp	Rejected recipients.
DrpMsg	Dropped messages.
SftBncEvnt	Soft bounced events.
CmpRcp	Completed recipients.

Statistic	Description
HrdBncRcp	Hard bounced recipients.
DnsHrdBnc	DNS hard bounces.
5XXHrdBnc	5XX hard bounces.
FltrHrdBnc	Filter hard bounces.
ExpHrdBnc	Expired hard bounces.
OtrHrdBnc	Other hard bounces.
DlvRcp	Delivered recipients.
DelRcp	Deleted recipients.
GlbUnsbHt	Global unsubscribe hits.
ActvRcp	Active recipients.
UnatmptRcp	Unattempted recipients.
AtmptRcp	Attempted recipients.
CrtCncIn	Current inbound connections.
CrtCncOut	Current outbound connections.
DnsReq	DNS requests.
NetReq	Network requests.
CchHit	Cache hits.
CchMis	Cache misses.
CchEct	Cache exceptions.
CchExp	Cache expired.
CPUTTm	Total CPU time used by the application.
CPUETm	Elapsed time since the application started.
MaxIO	Maximum disk I/O operations per second for the mail process.
RamUsd	Allocated memory in bytes.
SwIn	Memory swapped in.
SwOut	Memory swapped out.
SwPgIn	Memory paged in.
SwPgOut	Memory paged out.

Statistic	Description
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.
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 19: 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: XXXXXXXXXXX-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 .

Log Subscriptions

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 20: 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 4.
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 2.
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 4. 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 21: 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 2.

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 22: 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 26.

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 2.

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 28
- Rolling Over Logs Immediately via the CLI, on page 28

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 23: 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

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
```