

How to archive emails on the Email Security Appliance and Cloud Email Security?

Contents

[Introduction](#)

[Background Information](#)

[How to archive emails on the ESA and CES?](#)

[Configure Anti-Spam Archive](#)

[Configure Anti-Virus Archive](#)

[Configure Advanced Malware Protection Archive](#)

[Configure Graymail Archive](#)

[Configure Message Filter Archive](#)

[Validate Archive Mbox Logs Availability](#)

[Retrieve the Mbox Logs](#)

[Related Information](#)

Introduction

This document describes the steps to be followed in order to archive emails on the Email Security Appliance (ESA) and Cloud Email Security (CES) for retrieval and review.

Background Information

When you archive emails on the ESA and CES, it can be used to meet regulation requirements or to provide an additional means of data for further mail diagnosis and review. Archiving emails acts as a secondary storage of the emails in an mbox log format in it's original source for administrators in order to retrieve and validate.

- It is recommended to keep the settings to the default values if you decide to enable archiving of emails. The default values are 10MB per log and 10 logs maximum retained. The logs will continue to be added and rolled over based on the size of the log file itself. Archive mbox log files are filled based on the rate of the email traffic passing through the appliance. As more logs are created, older archive mbox logs are removed to free space for the creation of the new log.
- Ensure that your device has sufficient disk space before you increase the archive mbox log file sizes and maximum log files retained.
- In order to stop the archive mbox logs from being generated, you will have to disable the archive function per policy.

Note: ESA and CES archive mbox logs cannot be retrieved by the Security Management Appliance (SMA) and are stored locally per each ESA and CES with the feature enabled.




How to archive emails on the ESA and CES?

Email archiving is available with Anti-spam, Anti-virus, Advanced Malware Protection, Graymail and Message filters. The archive action can be configured through the graphical user interface (GUI) or command line interface (CLI) for Anti-spam, Anti-virus, Advanced Malware Protection and Graymail.

For message filters, the archive action can be configured using the CLI alone.


Configure Anti-Spam Archive

1. Navigate to the **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Click on the Anti-spam settings for the respective policy in order to configure email archiving.
3. Click **Advanced** on the available settings for Positively Identified Spam Settings and/or Suspected Spam settings.
4. Press the radio button next to Yes in order to archive emails with the respective Anti-spam verdict.
5. Submit the configuration, and commit these changes as shown in the image.

Positively-Identified Spam Settings									
Apply This Action to Message:	Spam Quarantine ▼ <i>Note: If local and external quarantines are defined, mail will be</i>								
Add Text to Subject:	Prepend ▼ [SPAM]								
▼ Advanced	<table border="1"> <tr> <td>Add Custom Header (optional):</td> <td>Header: <input type="text"/></td> </tr> <tr> <td></td> <td>Value: <input type="text"/></td> </tr> <tr> <td>Send to an Alternate Envelope Recipient (optional):</td> <td>Email Address: <input type="text"/> <i>(e.g. employee@compa</i></td> </tr> <tr> <td> Archive Message:</td> <td><input checked="" type="radio"/> No <input type="radio"/> Yes</td> </tr> </table>	Add Custom Header (optional):	Header: <input type="text"/>		Value: <input type="text"/>	Send to an Alternate Envelope Recipient (optional):	Email Address: <input type="text"/> <i>(e.g. employee@compa</i>	 Archive Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Add Custom Header (optional):	Header: <input type="text"/>								
	Value: <input type="text"/>								
Send to an Alternate Envelope Recipient (optional):	Email Address: <input type="text"/> <i>(e.g. employee@compa</i>								
 Archive Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes								

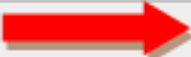
Configure Anti-Virus Archive

1. Navigate to the **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Click on the Anti-virus settings on the respective policy in order to configure email archiving.
3. On each of the scanning verdicts you wish to archive the original message, press the radio button next to Yes in order to archive.
4. Submit the configuration, and commit these changes as shown in the image.

Repaired Messages:	
Action Applied to Message:	Deliver As Is
 Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: VIRUS REMOVED]
▶ Advanced	Optional settings for custom header and message


Configure Advanced Malware Protection Archive

1. Navigate to the **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Click on the Advanced Malware Protection settings on the respective policy in order to configure the email archiving.
3. On each of the scanning verdicts you wish in order to archive the original message, press the radio button next to Yes in order to archive.
4. Submit the configuration, and commit these changes as shown in the image.

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
 Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
[WARNING: MALWARE DETECTED]	

Configure Graymail Archive

1. Navigate to the **GUI > Mail Policies > Incoming/Outgoing Mail Policies**.
2. Click on the Graymail settings on the respective policy in order to configure the email archiving.
3. Click **Advanced** on the available settings for Marketing, Social, Bulk.
4. Press the radio button next to Yes in order to archive emails with the respective Graymail verdict.
5. Submit the configuration, and commit these changes.

Action on Marketing Email	
Apply this action to Message:	Deliver ▼ Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [MARKETING]
▼ Advanced	Add Custom Header (optional): Header: <input type="text"/> Value: <input type="text"/>
	Send to an Alternate Envelope Recipient (optional): Email Address: <input type="text"/> (e.g. employee@)
	 Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes

Configure Message Filter Archive

Note: A message filter with archive action is required in order to view archived logs. Message filters can only be created within the CLI.

Sample filter:

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. Login to the device on the CLI.
2. Create a message filter as seen in the sample filter provided.
3. Submit this filter and commit your changes.

Validate Archive Mbox Logs Availability

When the configuration for archive is committed for the respective services, the archived emails are stored in an mbox format log file. In order to verify if the archive logs are available for retrieval, navigate to the **GUI > System Administration > Log Subscriptions**.

Security services archives create a separate log with an archive log type as shown in the image:

Configured Log Subscriptions			
Add Log Subscription...			
Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/ ←	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/ ←	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/ ←	None

For message filters the archive configuration is viewed from the **CLI only**:

• filters > logconfig

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
  Log Name      Log Type      Retrieval      Interval
  -----
  1. Test       Filter Archive Logs  Manual Download  None
```

Retrieve the Mbox Logs

For stand-alone appliances these mbox logs can be retrieved directly from GUI. Navigate to

the **GUI > System Administration > Log Subscriptions** and click on the **Log Files** for the respective archive log you will retrieve.

For clustered appliances, the mbox logs can be retrieved with the use of FTP/Secure Copy (SCP) as described in this [article](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00...). (<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00...>)

Related Information

- [Cisco Email Security Appliance - End-User Guides](#)
- [What is UNIX mbox \(mailbox\) format?](#)
- [Where are logs stored on the Cisco Email Security Appliance \(ESA\) and how do I access them](#)
- [How to extract an email from the archive mbox logs](#)
- [Technical Support & Documentation - Cisco Systems](#)