

# Message or Content Filter Scanning Error Matches Conditions and Takes Action

## Contents

[Introduction](#)

[Problem](#)

[Solution](#)

[Related Information](#)

## Introduction

This document describes why messages are matching Message or Content filter conditions when a "message scanning error" occurs on the Cisco Email Security Appliance (ESA) and Cloud Email Security (CES) appliance.

## Problem

Messages are sent into the ESA/CES for filtering, the mail\_logs or message tracking shows the results of "message scanning error" followed by a positive match against the message/content filter that was conducting the scan.

Sample errors found on the mail\_logs/message tracking:

```
Tue Sep 9 13:37:35 2014 Warning: MID 15180223, message scanning error: Size Limit Exceeded
Tue Sep 9 14:27:31 2015 Warning: MID 15180325, message scanning error: Scan Depth Exceeded
```

## Solution

When an email attachment exceeds a threshold configured, a message scanning error is logged. Should the ESA/CES have **assume the attachment matches** enabled, it will trigger the filter match and action as configured.

**Note:** Attachment scanning on the ESA/CES has different thresholds which are defined within the **scanconfig** configuration on the CLI or **scan behaviour** settings on the GUI.

On the CLI, the feature can be enabled or disabled in the **scanconfig** command:

```
myesa.loc> scanconfig
```

There are currently 5 attachment type mappings configured to be SKIPPED.

Choose the operation you want to perform:

- NEW - Add a new entry.

- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.

[>] setup

1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.

Choose one:

[2]>

Enter the maximum depth of attachment recursion to scan:

[5]>

Enter the maximum size of attachment to scan:

[2621440]>

Do you want to scan attachment metadata? [Y]>

Enter the attachment scanning timeout (in seconds):

[1]>

If a message has attachments that were not scanned for any reason (e.g. because of size, depth limits, or scanning timeout), assume the attachment matches the search pattern? [Y]>

Ensure all changes are committed by entering the **commit** command..

On GUI:

1. Navigate to **Security Services** then **Scan Behaviour**
2. Click **Edit the Global Settings**
3. Disable/Enable **Assume attachment matches pattern if not scanned for any reason.**

### Edit Scan Behavior

| Global Settings  |  |
|--|--|
| Action for attachments with MIME types / fingerprints in table above:        | <input type="radio"/> Scan <input checked="" type="radio"/> Skip                                       |
| Maximum depth of attachment recursion to scan:                               | <input type="text" value="5"/>   |
| Maximum attachment size to scan:   | <input type="text" value="5M"/><br><small>(Add a trailing K or M to indicate size units)</small>       |
| Attachment Metadata scan:  | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled                                |
| Attachment scanning timeout:   | <input type="text" value="30"/><br><small>(seconds)</small>  |
| Assume attachment matches pattern if not scanned for any reason:             | <input type="radio"/> Yes <input checked="" type="radio"/> No  |
| Assume zip file to be unscannable if files in the archive cannot be read?    | <input type="radio"/> Yes <input checked="" type="radio"/> No  |
| Action when message cannot be deconstructed to remove specified attachments: | <input checked="" type="radio"/> Deliver<br><input type="radio"/> Bounce<br><input type="radio"/> Drop |
| Bypass all filters in case of a content or message filter error:             | <input checked="" type="radio"/> Yes <input type="radio"/> No  |
| Encoding to use when none is specified:                                      | <input type="text" value="US-ASCII"/>  |
| Convert opaque-signed messages to clear-signed (S/MIME unpacking):           | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled                                |

For more information about the `scanconfig` command, see the AsyncOS Advanced User Guide on the [Cisco Support Portal](#).

## Related Information

- [Cisco Email Security Appliance - End-User Guides](#)
- [Technical Support & Documentation - Cisco Systems](#)
- [What does "Message Scanning Problem: Size Limit Exceeded" mean](#)