

Troubleshoot Messages in Multiple Quarantines

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[ComponentsUsed](#)

[Quarantine Types](#)

[Related Information](#)

Introduction

This document describes how a message on a Cisco Email Security Appliance (ESA) can reside in multiple quarantines. Quarantines are temporary mail repositories that hold messages for further processing.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Email Gateway AsyncOS version 16.x
- Policy, Virus, and Outbreak Quarantines

The information in this document was created from devices in a specific lab environment. All devices used in this document started with a cleared (default) configuration. If the network is live, ensure that the potential impact of any command is understood before the command is used.

Quarantine Types

Depending on the licensed features, a Cisco ESA can be initially configured with up to three quarantines.

- Outbreak - a quarantine used by Virus Outbreak Filters, created when the Virus Outbreak Filters license key is enabled.
- Virus - a quarantine used by the anti-virus engine, created when the anti-virus license key is enabled.
- Policy - a default quarantine (for example, you can use this to store messages requiring Legal review).
- File Analysis - holds messages that are sent for file analysis until a verdict is returned.

A message can end up in more than one quarantine for a variety of reasons. For example, a filter can be created to quarantine email that contains offensive material to the 'Policy' quarantine. If a received message matches that filter and also includes an encrypted attachment that cannot be scanned for viruses, the message is placed in both the 'Virus' and the 'Policy' quarantine.

Example message from the mail_logs:

```
Sat Jul 25 00:56:03 2026 Info: MID 14712 ready 1352 bytes from <user@example.com>
Sat Jul 25 00:56:03 2026 Info: MID 14712 attachment 'encryptedfile.zip'
Sat Jul 25 00:56:03 2026 Info: ICID 14971 close
Sat Jul 25 00:56:03 2026 Info: MID 14712 matched all recipients for per-recipient policy DEFAULT in the
Sat Jul 25 00:56:03 2026 Info: MID 14712 interim verdict using engine: CASE spam negative
Sat Jul 25 00:56:03 2026 Info: MID 14712 using engine: CASE spam negative
Sat Jul 25 00:56:03 2026 Info: MID 14712 interim AV verdict using Sophos ENCRYPTED
Sat Jul 25 00:56:03 2026 Info: MID 14712 antivirus encrypted
Sat Jul 25 00:56:03 2026 Info: MID 14712 quarantined to "Policy" (content filter:Quarantine)
Sat Jul 25 00:56:03 2026 Info: MID 14712 quarantined to "Virus" (a/v verdict:ENCRYPTED)
Sat Jul 25 00:56:03 2026 Info: Message finished MID 14712 done
```

Messages that reside in multiple quarantines are not delivered until they are released from all quarantines in which they reside.

Example release log:

The expected outcome is that the message is delivered only after it is released from both quarantines.

```
Sat Jul 25 00:57:00 2026 Info: MID 14712 released from quarantine "Virus" (manual) t=57
Sat Jul 25 00:57:49 2026 Info: MID 14712 released from quarantine "Policy" (manual) t=106
Sat Jul 25 00:57:49 2026 Info: MID 14712 released from all quarantines
```

Related Information

- [Cisco Secure Email Gateway - End-User Guides](#)
- [Cisco Technical Support & Downloads](#)