

The email flow is a series of stages that emails undergo once they are sent.

These steps are designed to filter and process emails, so they are delivered to the recipient's inbox in a secure manner.

Understanding each of these steps will help troubleshooting, optimizing, and securing your email systems.

email processing—sending, receiving, delivery, deferral, or failure.

Definition:

Logs provide a record of all email transactions.

Email logs are crucial for operational reliability, security, legal compliance, and effective email system management.

Email processing is maintained by MTA (Mail Transfer Agent):

Ubuntu native MTA's:

- **Postfix**
- **Exim**
- **Sendmail**
- **OpenSMTPD**

Windows native MTA's:

- **hMailServer**
- **MailEnable**
- **Microsoft Exchange Server**

Location of mail logs:

- `/var/log/mail.log` → **Main mail log**
- `/var/log/mail.err` → **Mail-related errors**
- `/var/log/mail.info` → **Informational messages**

Sample Log:

Jul 25 14:32:10 mailserver postfix/smtpd[12345]: connect from mail.example.com[192.0.2.1]

Jul 25 14:32:11 mailserver postfix/smtpd[12345]: 4F3C620C8A: client=mail.example.com[192.0.2.1]

Jul 25 14:32:12 mailserver postfix/cleanup[12346]: 4F3C620C8A: message-id=<1234567890@mail.example.com>

Jul 25 14:32:12 mailserver postfix/qmgr[12347]: 4F3C620C8A: from=<sender@example.com>, size=1024, nrcpt=1 (queue active)

Jul 25 14:32:13 mailserver postfix/smtp[12348]: 4F3C620C8A: to=<recipient@example.org>, relay=mx.example.org[198.51.100.2]:25, delay=1.5, delays=0.1/0.01/0.8/0.6, dsn=2.0.0, status=sent (250 OK id=abcdef12345)

Jul 25 14:32:14 mailserver postfix/smtpd[12345]: disconnect from mail.example.com[192.0.2.1]

Email Log Format :

- **Timestamp:** Jul 25 14:32:10
- **Hostname:** mailserver
- **Process and PID:** postfix/smtpd[12345]
- **Queue ID:** 4F3C620C8A (unique per email message)
- **Client info:** mail.example.com[192.0.2.1] (sending server's hostname and IP)
- **Message ID:** <1234567890@mail.example.com>
- **Sender:** from=<sender@example.com>
- **Recipient:** to=<recipient@example.org>
- **Relay:** where mail is sent next (mx.example.org[198.51.100.2]:25)
- **Status:** status=sent (250 OK id=abcdef12345) — indicates successful delivery
- **Delays:** Breakdown of time spent in various steps (queue, connection, transmission)

All the above parameters are almost the same for Postfix Logs, Sendmail Logs, Qmail

Possible status:

- **2xx** = Email sent successfully.
Status = sent
- **4xx** = Temporary problem, server will try again later.
Status = deferred
 - Insufficient system storage
 - Local error in processing
 - Mailbox unavailable
 - Service not available
- **5xx** = Permanent failure, email bounced back or rejected.
Status = bounced, discarded

Uses of Mail log:

- Troubleshooting email delivery problems
- Monitoring incoming/outgoing messages
- Diagnosing server or relay issues
- Verifying spam