



AMG

AIR-GAP MAIL GATEWAY



2U RACK-MOUNT APPLIANCE

Mail flow and queue: the rules of an unambiguous relay

Where each message enters, where it waits, when it is delivered and what happens if it is not, all by explicit rule and never by guesswork.

For: Mail administrators**In this catalog:** The nine fixed rules, the life of a message, durability, the queue, settings, and what happens when something fails<https://www.bardin.tech/en/bardingate-amg/>

AMG is a transparent relay, and transparency means no decision that depends on content or names. Direction, destination and fate follow from a few simple rules, each of which can be tested.



⚡ Your two networks stay separate and are never physically connected to each other; the 2U rack-mount appliance is attached to only one of them at any moment.

☰ Nine fixed rules

- 1 **Exactly one MTA** is configured on each network.
- 2 **The two IPs differ.** The Safe and Unsafe peers cannot share an address.
- 3 **Both connect directly.** NAT, load balancers, SMTP proxies and forwarded-source headers are outside this release.
- 4 **Only those two IPs may submit mail.** AMG is never an open relay.
- 5 **Recipient, sender, domain, headers and body never select direction.** It comes only from the connecting peer's IP.
- 6 **A multi-recipient envelope stays whole** and goes to the opposite MTA; it is not split by recipient domain.
- 7 **Content is not modified.** Only the standard Received trace header is added.
- 8 **A permanent failure creates a standard DSN** routed back to the originating MTA, not toward the failed destination.
- 9 **This release runs no mailbox, content inspection, scanning, SPF/DKIM/DMARC policy or recipient validation.**

Direction is the IP, and nothing more

A message with forged headers or an odd recipient cannot change its direction, because direction is read from the direct TCP peer's address, and only two addresses are allowed.

A successful transfer, step by step

1

The peer connects

The source MTA connects and passes that side's security profile: permitted IP, TLS and, if configured, mTLS or AUTH.

2

Durable acceptance

Postfix accepts the whole SMTP transaction into persistent spool, then returns 250.

3

Safe keeping

The message is recoverable across a restart and an abrupt power loss.

4

Attempt at the destination

Postfix sends the same message to the opposite MTA at its configured IP and port.

5

Delivered

On downstream success the state becomes Delivered and the payload follows the configured retention.

6

Record and event

Redacted metadata and audit are recorded and a structured event goes to your SIEM.

The life of a message

Accepted → Durably queued → Delivered

Deferred

Failed: DSN

Expired: DSN

Deferral is temporary and carries a stable, redacted reason and the next attempt time; failure and expiry are terminal and both notify the sender.

State	What happens
Accepted	SMTP 250 is returned only after Postfix has durably accepted the message under the configured filesystem durability profile.
Deferred	Bounded, persistent retry. Retry Now asks for one extra attempt but never bypasses routing, TLS, admission, capacity or switching controls.
Delivered	The payload follows the configured retention; queue metadata stays.
Failed or expired	A standard DSN to the originating MTA, with a warning before expiry. No silent deletion is permitted.

Durability

- An accepted, undelivered message survives a process or container restart, a host reboot, an abrupt power loss and **one physical disk failure**; persistent storage and the appliance's RAID provide this, encrypted.
- The moment of acceptance is the moment of durability, so no message is acknowledged and then lost.

Capacity pressure and maintenance

- **The undelivered queue is never deleted to relieve pressure.** Retained delivered payload goes first, oldest first; if protected capacity is still short, new admission returns a temporary 4xx and the sender's MTA retries later.
- **Maintenance and updates:** new admission pauses with 4xx, open SMTP transactions reach a safe boundary, the queue is preserved, the update is applied and health verified, then it resumes or rolls back.

Why 4xx rather than dropping

A temporary 4xx tells the sending MTA to keep the message and try later, so the appliance is never where a message is lost. Deleting mail to make room would turn AMG into the point of loss.

Settings and defaults

Setting	Default	Note
Queue lifetime	5 days	Adjustable within safe bounds; a warning before expiry
Message size	50 MiB	Configurable
Delivered payload	Removed after delivery	Can be kept for a duration under an explicit storage cap
Queue metadata	One year	Configurable within safe ranges
Security audit	Five years	Configurable within safe ranges
Retry and concurrency	Conservative	Curated settings; raw Postfix keys are never exposed

There is no artificial licence cap on throughput, domains, recipients or queue entries; limits follow the validated hardware and storage.

Applying a setting: stepwise and reversible



After a crash at any step, the state is rebuilt from the active configuration version, the generated file's digest and observation of the runtime and queue. Postfix files are derived, never the source.

When something fails

Situation	Behaviour
Unknown peer, or the same IP configured twice	Refused; mail is not accepted, the configuration does not activate
Invalid TLS identity or a required secret is missing	No connection; no fall back to a weaker mode
Ambiguous direction or malformed configuration	Rejected before apply
Postfix, runtime or SIEM failure	An accepted message is never reported delivered; a SIEM fault never blocks SMTP

What is tested

- Both directions with one and several recipients, and proof that changing recipient, domain or headers never changes direction.
- No DNS query during relay; TLS required, opportunistic and off, with optional mTLS and AUTH.
- Power loss and restart around the 250 reply, configuration activation, delivery and cleanup; and disk pressure.
- No payload, subject or secret in logs, database, diagnostics or SIEM.

✦ How much work is it for you?

You enter two IP addresses, ports and, if you want them, certificates, then press Apply. The rest, the queue, retries, DSNs and events, runs by itself.

An accepted message is either delivered or ends in a standard, visible way; there is no third outcome.

More about this product

CATALOG 1
Product overview

CATALOG 3
Security and isolation

CATALOG 4
Operations and integration

For advice, a demonstration and contact details:
<https://www.bardin.tech/en/bardingate-amg/>



Specifications may change without notice.