Modern-auth relay for legacy devices

Administrator Manual

SMTP-365 documentation

Modern-auth relay for legacy devices

SMTP-365: Administrator Manual

Day-to-day operation of an installed relay. For installation see the Installation Guide; for internals see the Technical Specification.

0. The System pages (appliance)

On an appliance the **System** menu manages the host itself; on a manual Debian install without the system agent these pages show what they can and explain what must be done by hand.

Page	What it does
Overview	Version, addresses, uptime, disk and memory, service states, restart services, reboot, shut down
Network & time	Hostname, time zone, DHCP or static address (systemd-networkd)
Relay & firewall	SMTP port and banner, subnets allowed to submit scans, subnets allowed to reach this interface, SharePoint pseudo-domain, unmapped-address action, recipient domain allow-list, retry policy, log level. Saving rewrites the firewall and restarts the SMTP service
Licence	Current state, enter or replace a key
HTTPS certificate	Issue a new self-signed certificate or upload your own PEM certificate and key; nginx reloads without downtime
Software update	Upload a signed `.smtp365-update` bundle; it is verified, shown for confirmation, installed, and services restart
Backup & restore	Download an archive of settings, routes, credentials, certificate and firewall; restore one (optionally including the IP configuration)
Logs	Journal of each service, downloadable for support

Microsoft 365 (top menu) shows the connected tenant and app, tests the connection, and can re-run the automatic onboarding or take manual values. The optional Exchange PowerShell snippet that limits sending to the scanner mailbox is shown there too.

Licence states: *licensed* (no banner), *evaluation* (banner with days remaining), *expired* (scans are accepted and held until a key is entered; nothing is lost). The web admin password also unlocks root on the console and over SSH.

1. How scans flow

1 A user picks a destination on the printer and scans.

2 The printer emails the scan to the relay over SMTP.

3 The relay saves the message to its spool and tells the printer "accepted".

4 Within a second or two the relay delivers it:

5 to a **normal email address**: sent through Microsoft 365 from the

scanner mailbox (or the printer's own From address, if the override is off);

- to `<name>@sharepoint.local`: converted to PDF if needed and uploaded

to the folder mapped to `<name>`.

1 If Microsoft is temporarily unavailable, the relay retries for about an

hour. If delivery is impossible, the scan is kept and you receive an alert email.

Nothing is deleted until it has been delivered or you discard it.

2. The web interface

Open `http://<relay-ip>:8080/` from a PC on an allowed subnet and sign in. There is one account, `admin`.

2.1 Routes

Lists every `@sharepoint.local` address and the library and folder it delivers to.

Add route: enter the local part (letters, digits, dots, dashes or underscores; the domain is fixed), an optional description, then pick the folder:

- The **Document library** drop-down lists every library on the configured

site.

- The tree below shows folders. Click a folder to select it; click the arrow

or double-click to expand. The library root itself can be selected.

- **New folder here** creates a subfolder inside the selected folder.
- The selection is shown above the tree. Save.

The route is live immediately. Editing a route re-opens the picker with the current selection; deleting one makes the address unmapped (see 2.5).

Ordinary email addresses never need a route.

2.2 Settings

Microsoft Graph: tenant id, client id and client secret. If these are supplied by the server's environment file they appear read-only with a "from environment" tag. The secret is never displayed; leave the field blank to keep the existing one.

SharePoint: the site URL. On save it is resolved to a site id through Graph and the resolved name is shown. Routes can only target this site.

Scan-to-email sender:

- *Override sender address* unticked: emails are sent from whatever From

address the printer used. That mailbox must be covered by the Exchange access policy.

- Ticked: every scan email is sent from the fixed mailbox entered below,

regardless of the printer. Recommended.

Alerts: the address that receives failure and held-scan notifications, and the mailbox they are sent from. The alert sender is also the fallback From address when a scan has none and the override is off.

Test Graph connection acquires a token and reports the application's name and granted permissions, plus the configured site. It warns if `Mail.Send` or a `Sites.*` permission is missing. It sends and writes nothing.

The read-only panel at the bottom shows the server-side configuration from `config.yaml` (listen addresses, size limit, retry policy, paths).

2.3 Status & logs

Top row: Graph token state (valid, with time to expiry; not cached until first use; or not configured), pending/retrying count, held count, failed count, and total successes in the job log.

Then, when present, tables of **held**, **failed** and **pending/retrying** jobs with the sender, recipients, subject, attempt count, next attempt time and last error. Each has:

- **Re-queue**: puts the scan back at the front of the queue with the

attempt counter reset. Use after fixing the cause (adding a route, restoring connectivity, fixing credentials).

- **Discard**: deletes the scan permanently.

Finally **Recent jobs**: the last 200 jobs with time, source IP, from/to, subject, file count, size, action, status and any error detail. Statuses:

Status	Meaning
`pending`	Accepted, waiting for the worker
`retrying`	A transient error occurred; will retry at the shown time
`success`	Delivered
`failed`	Retries exhausted or a permanent error; kept in the failed queue
`held`	Sent to an unmapped `@sharepoint.local` address; kept in the held queue
`rejected`	Refused at SMTP time (too large, unparsable, disallowed recipient) or discarded by an admin; nothing kept

2.4 Password

Change the admin password at any time: current password, new password twice. Minimum 10 characters with letters and digits; common passwords and the default are refused. On a fresh install this page is enforced before anything else can be used.

2.5 Held scans (unmapped addresses)

If someone scans to `finance@sharepoint.local` before that route exists, the relay accepts the scan, holds it, and emails the alert address. To deliver it: add the route on the Routes page, go to Status, and click **Re-queue** on the held job. It uploads within the poll interval (30 seconds by default).

If you would rather printers get an immediate error for unknown addresses, set `routing.unmapped_action: reject` in `config.yaml` and restart `mfp-relay`. Held jobs already in the queue are unaffected.

2.6 Failed scans

A job fails after five attempts against a transient problem, or immediately on a permanent one (for example `403 ErrorAccessDenied` because the sender mailbox is not allowed, or a route that was deleted while a job was waiting). The alert email includes the job id and error. Fix the cause, then Re-queue from the Status page. The original message is kept intact in `/var/spool/mfp-relay/failed/`.

3. Command-line tools

All live in `/opt/mfp-relay/venv/bin/`. Run them as root; they read the same config and environment file as the services.

Command	Use
`mfp-relay-admin test-graph`	Verify credentials and permissions. Exit code 1 if a permission is missing.

Command	Use
`mfp-relay-admin settings show`	Print all settings (secrets masked).
`mfp-relay-admin settings set key=value …`	Change settings without the UI, e.g. `sender_override_enabled=0`.
`mfp-relay-admin settings resolve-site URL`	Change the SharePoint site. Existing routes pointing at the old site keep working only if the app still has access to it.
`mfp-relay-admin reset-password [--final]`	Recover a lost admin password. Without `--final`, a change is forced at next login.
`mfp-relay-admin send-test ADDRESS [--file F]`	Submit a test message through the local SMTP port.
`mfp-relay-admin run-due`	Process due retries once (the service does this automatically).
`mfp-relay-admin show-config`	Dump the effective configuration as JSON.

Service control:

```
systemctl status mfp-relay mfp-relay-web
systemctl restart mfp-relay            # after editing config.yaml
journalctl -u mfp-relay -u mfp-relay-web -f
```

4. Logs

`/var/log/mfp-relay/relay.log` holds one JSON object per line and is rotated daily with 30 days kept. Examples of useful queries:

```
# everything about one job
grep '"job_id": "c8d4f2b3' /var/log/mfp-relay/relay.log

# failures today
grep '"status": "failed"' /var/log/mfp-relay/relay.log

# who is scanning, from where
grep '"job accepted"' /var/log/mfp-relay/relay.log | jq -r '[.ts, .source_ip, .mail_from, (.recipients|join
```

The same messages, in plain text, go to the journal.

5. Configuration files

File	Contents	After editing
`/etc/mfp-relay/config.yaml`	Listen addresses, ports, allowed subnets, size limit, retry policy, SharePoint pseudo-domain, unmapped action, recipient allow-list, paths	`systemctl restart mfp-relay mfp-relay-web`
`/etc/mfp-relay/mfp-relay.env`	Tenant id, client id, client secret (optional; overrides the UI)	`systemctl restart mfp-relay mfp-relay-web`
`/etc/nftables.d/mfp-relay.nft`	Firewall rules for the two ports	`nft -f /etc/nftables.conf`
`/var/lib/mfp-relay/mfp-relay.sqlite3`	Settings entered in the UI, routes, admin account, job log	Nothing; read live

To change the relay IP or the allowed subnets, re-run `deploy/configure-server.sh` with new values; it rewrites `config.yaml` and the firewall rules and backs up the previous config.

5.1 Restricting email recipients

By default a scan can be emailed to any address, internal or external. To limit it to your own domains:

```
routing:
  allowed_recipient_domains: [yourdomain.com, yourdomain.onmicrosoft.com]
```

Other recipients are refused at SMTP time with `550 5.7.1`, which the printer displays as an error. Exchange transport rules and DLP policies also apply to relay-sent mail exactly as to any other mail from that mailbox.

5.2 Message size

`smtp.max_message_bytes` (25 MB default) is checked before anything is stored. Emails with attachments over 3 MB and uploads over 4 MB are handled automatically with Graph upload sessions, so the only ceiling is this setting and the mailbox's own limits.

6. Backup and restore

Back up:

- `/etc/mfp-relay/` (config and credentials)
- `/var/lib/mfp-relay/mfp-relay.sqlite3` (routes, settings, admin login, job history). Copy it with `sqlite3 /var/lib/mfp-relay/mfp-relay.sqlite3 ".backup /path/backup.sqlite3"` for a consistent snapshot while the services run.
- Optionally `/var/spool/mfp-relay/` if undelivered scans matter.

Restore by installing the software on a new server, copying those paths back with the same ownership (`root:mfp-relay 0640` for the env file, `mfp-relay:mfp-relay 0600` for the database), and restarting the services. The Microsoft 365 side needs no change as long as the same app registration is used.

7. Rotating credentials

Credential	How
Graph client secret	Run `Register-MfpRelayApp.ps1` again with the real site and mailboxes (without `-SkipCredential`), install the new `mfp-relay.env`, restart both services, run `test-graph`, then delete old secrets in the Entra portal under the app's Certificates & secrets. Secrets created by the script last 24 months; diary the expiry.
Web admin password	Password page in the UI, or `mfp-relay-admin reset-password --final`.
Web session key	`sqlite3 /var/lib/mfp-relay/mfp-relay.sqlite3 "delete from settings where key='web_secret_key'"` then restart `mfp-relay-web`; a new key is generated and all sessions are signed out.
Server root password / SSH keys	Standard Debian practice; the relay does not depend on them.
GitHub deploy key	Generate a new key on the server, add it to the repository, remove the old one.

8. Troubleshooting

Symptom	Check
Printer says it sent, nothing arrives	Status page: is the job `retrying` or `failed`? Read the detail column. If no job appears at all, the printer never reached the relay: check firewall and `smtp.allowed_sources`.

Symptom	Check
Job `failed` with `ErrorAccessDenied`	The From mailbox is not in the Application Access Policy, or the policy has not propagated. Turn on sender override, or add the mailbox to the "MFP Relay Senders" group.
Job `failed` with `itemNotFound` on upload	The target folder was deleted or moved in SharePoint. Edit the route and pick the folder again, then Re-queue.
Token state "Not configured"	Tenant/client id missing. Settings page or env file.
Test connection fails with `invalid_client`	Wrong or expired secret.
Test connection warns of missing permissions	Consent not granted; re-run the registration script or grant in the portal.
Folder picker shows "unavailable"	Site not resolved, or `Sites.Selected` grant missing on that site.
Scans arrive as many single-page files instead of one PDF	The printer is sending one email per page. Change its scan setting to "multi-page" or "one file".
Uploaded PDF has blank or black pages	Unusual TIFF encoding; send the scan as JPEG or PDF from the printer instead.
Many `550 5.7.1 Relaying denied` in the log	An unexpected device is attempting to use the relay. Investigate the source IP.
Web UI unreachable from a PC	Its subnet is not in `WEB_SUBNETS`; the login page is also throttled after 10 failed attempts per IP for 5 minutes.
Service keeps restarting at boot	Usually the LAN address arriving late from DHCP; it settles once the lease lands. Check `journalctl -u mfp-relay -b`.

9. Routine maintenance

- Glance at the Status page weekly, or rely on alert emails.
- Diary the client secret expiry (24 months from creation).
- Keep the server patched (`apt-get upgrade`) and pull relay updates occasionally (`git pull && deploy/install.sh && systemctl restart mfp-relay mfp-relay-web`).
- The job log prunes itself to the newest 5000 entries; the spool holds only undelivered scans; logs rotate automatically. No other housekeeping is required.