



Modern-auth relay for legacy devices

Installation Guide

SMTP-365 documentation

Modern-auth relay for legacy devices

SMTP-365: Installation Guide

Two ways to install:

- **Appliance (recommended, 0.2.0+)**: deploy a ready-made virtual machine image or boot the installer ISO, then do everything else in a browser. Section A.
- **Manual on an existing Debian server**: the scripted install used for version 0.1.0. Section B onwards (sections 1 to 8).

A. Appliance installation

A.1 Deploy

Platform	File	Notes
VMware ESXi / Workstation / VirtualBox	<code>smtp365-<version>-amd64.ova</code>	Import; 1 vCPU, 2 GB RAM, 16 GB thin disk preset
Hyper-V	<code>smtp365-<version>-amd64.vhdx</code>	Generation 2, Secure Boot off or "Microsoft UEFI Certificate Authority"; 2 GB RAM
Proxmox / KVM	<code>smtp365-<version>-amd64.qcow2</code>	UEFI or BIOS; VirtIO disk and network
Bare metal or any hypervisor	<code>smtp365-<version>-amd64.iso</code>	Boots and erases the first disk unattended, then reboots into the appliance. Needs internet access during install for Debian packages

Attach the VM to the LAN that the printers use. The disk grows automatically on first boot if you enlarge it.

A.2 First boot

The console shows the address to browse to, for example <https://192.168.1.57/>. The certificate is self-signed at this stage, so accept the browser warning. Sign in as `admin` / `changeme`.

A.3 Setup wizard

- 1 **Admin password.** Also becomes the console and SSH root password.
 - 2 **Network.** Hostname, time zone, and optionally a static address (DHCP with a reservation on your router is equally good).
 - 1 **Relay & firewall.** SMTP port for the printers (2525, or 25 if the printer cannot change it), the subnets allowed to submit scans, the subnets allowed to open this web interface, the SharePoint pseudo-domain, what to do with scans to unmapped addresses, and optionally an allow-list of email recipient domains.
 - 1 **Licence.** Paste your key, or continue the 30-day evaluation.
 - 2 **Microsoft 365.** Enter the SharePoint site URL and click *Connect*.
- You are given a code to enter at microsoft.com/devicelogin and asked to sign in as a Global Administrator; the appliance then creates its own application in your tenant with only `Mail.Send` and `Sites.Selected`, consents it, and grants the one site. If automatic setup is not offered, use manual entry with values from `deploy/Register-MfpRelayApp.ps1`.
- 1 **Sender & alerts.** The scanner mailbox every scan email is sent from

(a shared mailbox works and needs no licence), and where alerts go.

- 1 **Finish.** Then add routes and configure the printers (sections 3.6, 4).

Optional but recommended: restrict the app to the scanner mailbox with the Exchange PowerShell snippet shown on the Microsoft 365 page.

Everything the wizard sets is editable later under **System** and **Settings**. A backup can be downloaded from System → Backup.

B. Manual installation on Debian

This path takes a fresh Debian server and a Microsoft 365 tenant to a working relay in about an hour, most of it waiting for module installs and browser sign-ins.

1. Before you start

Gather:

Item	Example	Notes
Server LAN IP	192.168.3.5	Static, or a DHCP reservation
Subnets that may reach the relay	192.168.1.0/24 192.168.3.0/24	Printers and admin PCs
SMTP port the printer can use	2525 (or 25)	Check the printer's scan settings
SharePoint site URL	https://tenant.sharepoint.com/sites/Scans or https://tenant.sharepoint.com	The root site URL is valid; libraries are picked later
Scanner mailbox	scanner@yourdomain	Can be created as a shared mailbox by the setup script
Admin alert address	it@yourdomain	Receives failure/held notifications
Global Administrator sign-in		For the one-time Microsoft 365 setup

Server requirements: Debian 12 or 13 with network access to GitHub (for the clone), PyPI (for Python packages) and Microsoft (login.microsoftonline.com, graph.microsoft.com) over HTTPS.

2. Microsoft 365 setup

Do this on a Windows PC with PowerShell (5.1 or 7). It creates the application identity the relay uses and restricts what it can do.

2.1 Scripted (recommended)

Clone or download the repository on the PC, then in `deploy\`:

```
powershell -ExecutionPolicy Bypass -File .\Register-MfpRelayApp.ps1 `
  -SiteUrl https://<tenant>.sharepoint.com/sites/<Site> `
  -SenderMailboxes scanner@<yourdomain> `
  -AdminEmail it@<yourdomain> `
  -CreateSharedMailbox `
  -EnvFileOut .\mfp-relay.env
```

Run it as a file, not by pasting into a console. What it does:

- 1 Installs the Microsoft.Graph and ExchangeOnlineManagement modules for your

user if missing.

- 1 Signs you in to Graph in a browser and resolves the site URL (fails before making changes if the URL is wrong).
- 1 Creates the app registration "MFP Scan Relay" with application permissions `Mail.Send` and `Sites.Selected`, creates its service principal and grants admin consent.
- 1 Creates a client secret valid for 24 months and prints it in yellow. Copy it; it is shown once.
- 1 Grants the app write access to the one site.
- 2 Signs you in to Exchange Online, creates any missing sender mailbox as a shared mailbox (with `-CreateSharedMailbox`), puts the sender mailboxes in a mail-enabled security group "MFP Relay Senders", and creates an Application Access Policy so the app can send only as those mailboxes.
- 1 Writes `mfp-relay.env` with the tenant id, client id and secret.

Useful options: `-WhatIf` previews every change; `-UseCertificate` uses a self-signed certificate instead of a secret (PowerShell 7 only) and writes the PEM key for the server; `-SitesPermission ReadWriteAll` requests the broader SharePoint permission; `-SkipCredential` (optionally with `-ClientSecret`) re-runs without minting another secret; `-SkipExchangePolicy` omits the mailbox restriction.

The access policy takes up to 30 minutes to become effective.

2.2 Manual equivalent

If you prefer the portal, the steps are in the README's section 1: register the app, add the two application permissions and grant consent, create a secret, grant the app to the site with a `POST /sites/{id}/permissions` call, and create the Exchange access policy with `New-ApplicationAccessPolicy`.

3. Server installation

All commands as root.

3.1 Get the code

The repository is private, so the server needs read access. A read-only deploy key is the cleanest option:

```
apt-get update && apt-get install -y git
ssh-keygen -t ed25519 -N "" -f /root/.ssh/id_ed25519 -C "mfp-relay-server"
cat /root/.ssh/id_ed25519.pub
```

Add the printed public key at the repository's Settings → Deploy keys (leave write access off), then:

```
ssh-keyscan github.com >> /root/.ssh/known_hosts
git clone git@github.com:<owner>/<repo>.git /usr/local/src/mfp-relay
cd /usr/local/src/mfp-relay
```

3.2 Configure and install in one step

Edit the values at the top of `deploy/configure-server.sh` (relay IP, local subnets, ports), or pass them as environment variables, then run it:

```
RELAY_IP=192.168.3.5 \
LOCAL_SUBNETS="192.168.1.0/24 192.168.3.0/24" \
SMTP_PORT=2525 \
```

deploy/configure-server.sh

The script:

- 1 Warns if the relay IP is not present on an interface (harmless if it is about to arrive from DHCP).
 - 1 Installs git, nftables, Python and the application into a virtualenv at `/opt/mfp-relay/venv` via `deploy/install.sh`, creating the `mfp-relay` system user, `/var/lib/mfp-relay`, `/var/spool/mfp-relay`, `/var/log/mfp-relay`, both systemd units and the logrotate rule.
 - 1 Writes `/etc/mfp-relay/config.yaml` for the given IP, port and subnets (backing up any existing file).
 - 1 Writes nftables rules to `/etc/nftables.d/mfp-relay.nft`, includes them from `/etc/nftables.conf`, syntax-checks and loads them, and enables the nftables service. Only the listed subnets can reach the SMTP and web ports; nothing else on the host is affected.
 - 1 Enables and starts `mfp-relay` and `mfp-relay-web`.
- Other overridable variables: `WEB_PORT`, `SMTP_SUBNETS`, `WEB_SUBNETS` (narrow the SMTP or web audience separately), `SHAREPOINT_DOMAIN`, `MAX_MESSAGE_MB`.

3.3 Install the Graph credentials

Copy the `mfp-relay.env` produced in step 2 to the server (for example with `scp`), then:

```
install -m 0640 -o root -g mfp-relay mfp-relay.env /etc/mfp-relay/mfp-relay.env
systemctl restart mfp-relay mfp-relay-web
/opt/mfp-relay/venv/bin/mfp-relay-admin test-graph
```

Expected output ends with `Granted roles: Mail.Send, Sites.Selected`. Delete the copy of `mfp-relay.env` on the PC.

Alternatively, leave the env file out and enter the tenant id, client id and secret on the web UI's Settings page; they are stored in the database instead. The env file wins if both are present.

3.4 Set the site and sender policy

Either on the Settings page of the web UI, or from the shell:

```
A=/opt/mfp-relay/venv/bin/mfp-relay-admin
$A settings resolve-site https://<tenant>.sharepoint.com/sites/<Site>
$A settings set admin_alert_email=it@<yourdomain> alert_sender_upn=scanner@<yourdomain> \
    sender_override_enabled=1 sender_override_upn=scanner@<yourdomain>
$A test-graph
```

Turning the sender override on is recommended: every scan email then comes from the scanner mailbox regardless of what the printer puts in its From field, and only that mailbox needs to be in the access policy.

3.5 First login and admin password

Browse to `http://<relay-ip>:8080/` from a PC in an allowed subnet. Sign in as `admin / changeme`. You are taken to the password page and cannot open any other page until you set a new password (at least 10 characters with letters and digits; common passwords are refused).

To set the password from the shell instead, and skip the forced change:

```
/opt/mfp-relay/venv/bin/mfp-relay-admin reset-password --final
```

3.6 Add SharePoint routes

On the Routes page click **Add route**, type the local part (for example `accounting`), choose the document library, expand the tree and select the destination folder, and save. `accounting@sharepoint.local` is live immediately. Create folders from the picker with **New folder here** if needed.

4. Configure the printer

Setting	Value
SMTP server	the relay's LAN IP
Port	as configured (2525 by default)
Authentication	none
SSL/TLS/STARTTLS	off
Sender / device email address	the scanner mailbox (only matters when sender override is off)
Scan file format	PDF where offered; TIFF/JPEG are converted for SharePoint destinations
Address book entries	staff addresses for email; <code><name>@sharepoint.local</code> for folders

Some printers validate that the SMTP server "accepts" the sender with a test button; that works. Some insist on port 25; set `SMTP_PORT=25` when running `configure-server.sh` (no extra privileges are needed).

5. Verify

From the server:

```
A=/opt/mfp-relay/venv/bin/mfp-relay-admin
$A send-test you@<yourdomain> # email path
$A send-test accounting@sharepoint.local --file sample.tif # SharePoint path (route must exist)
tail -n 5 /var/log/mfp-relay/relay.log
```

Each should log `job accepted` followed by `job completed` with `"status": "success"`. Then repeat from the printer itself. The Status page shows every job, its outcome and any error text.

Suggested acceptance tests:

- 1 PDF scan to a mailbox: arrives with the attachment intact.
- 2 Image scan to a SharePoint route: one PDF appears in the chosen folder.
- 3 Disconnect the server's internet briefly mid-scan: Status shows `retrying`; the scan delivers when connectivity returns.
- 1 Scan a file larger than the limit: printer reports an error; Status shows `rejected`.
- 1 Connect from an address outside the allowed subnets: the connection is dropped by the firewall.
- 1 Add a new route in the UI and scan to it without restarting anything.
- 2 Confirm the forced password change on a fresh install.

6. Upgrading

```
cd /usr/local/src/mfp-relay && git pull && deploy/install.sh
```

```
systemctl restart mfp-relay mfp-relay-web
```

`install.sh` never overwrites `config.yaml` or the env file. If the server shows "local changes would be overwritten" on pull, the only local change will be a file mode; discard it with `git checkout -- deploy/` first.

7. Uninstalling

```
systemctl disable --now mfp-relay mfp-relay-web
rm -f /etc/systemd/system/mfp-relay.service /etc/systemd/system/mfp-relay-web.service
systemctl daemon-reload
rm -rf /opt/mfp-relay /etc/mfp-relay /var/lib/mfp-relay /var/spool/mfp-relay /var/log/mfp-relay
rm -f /etc/logrotate.d/mfp-relay /etc/nftables.d/mfp-relay.nft
sed -i '/mfp-relay.nft/d' /etc/nftables.conf && nft -f /etc/nftables.conf
userdel mfp-relay
```

In Microsoft 365, delete the app registration, the "MFP Relay Senders" group and the Application Access Policy, and remove the site permission.

8. Installation troubleshooting

Symptom	Cause and fix
<code>git: command not found</code>	<code>apt-get install -y git</code>
<code>Permission denied (publickey)</code> on clone	Deploy key not added, or added to the wrong repository
Service <code>activating (auto-restart)</code> and journal shows <code>could not bind on any address</code>	<code>config.yaml</code> bind address is not on this host; re-run <code>configure-server.sh</code> with the right <code>RELAY_IP</code>
Journal shows <code>unable to open database file</code>	The database was created by a root-run command before the fix in 0.1.0 was installed; <code>chown -R mfp-relay:mfp-relay /var/lib/mfp-relay</code>
<code>test-graph: tenant ID / client ID not configured</code>	Env file missing or unreadable; check <code>/etc/mfp-relay/mfp-relay.env</code> permissions
<code>test-graph: AADSTS7000215 Invalid client secret</code>	Wrong or expired secret; re-run the registration script without <code>-SkipCredential</code>
<code>test-graph: Insufficient privileges</code> reading the site	Site grant missing (Sites.Selected); re-run the script with <code>-SkipCredential</code>
Send fails with 403 <code>ErrorAccessDenied</code>	Sender mailbox not covered by the Application Access Policy, or the policy has not propagated yet (up to 30 minutes)
Printer reports connection refused	Firewall: printer subnet not in <code>SMTP_SUBNETS</code> ; check <code>nft list table inet mfp_relay</code>
Printer reports <code>550 5.7.1 Relaying denied</code>	Printer IP not in <code>smtp.allowed_sources</code> in <code>config.yaml</code>