Modern-auth relay for legacy devices

Product Overview

SMTP-365 documentation

Modern-auth relay for legacy devices

SMTP-365: Product Overview

Version 0.2.0

SMTP-365 ships as a ready-to-run appliance: a virtual machine image (VMware, Hyper-V, Proxmox) or a bootable installer ISO. After booting, everything is configured from a browser through a guided setup wizard, including the connection to Microsoft 365. It is licensed per appliance with a perpetual key and an optional maintenance period for updates, and includes a 30-day evaluation mode out of the box.

The problem

Multi-function printers (MFPs) are the most visible example, but they are far from alone. Uninterruptible power supplies, server management controllers (HP iLO, Dell iDRAC), network-attached storage, phone systems and PBXs, alarm and building-management panels, and countless monitoring and line-of-business tools all send scans, reports or alerts by email over legacy SMTP: plain or no authentication, and often no TLS.

Microsoft 365 no longer accepts that. Basic authentication for SMTP submission has been retired, and Exchange Online expects modern (OAuth2) authentication that these devices cannot perform. Overnight, scan-to-email stops working and alert emails silently vanish, with no practical way to point the hardware at Microsoft 365 directly.

The product

SMTP-365 is a small, self-contained relay that runs inside the office network. It accepts email from legacy devices over plain SMTP, exactly as they expect, and delivers it to Microsoft 365 through the Microsoft Graph API using a properly secured application identity. Most devices need a single settings change, point SMTP at the relay, and never need touching again.

Each message is delivered in one of two ways, decided by the address the device sends to:

Address sent to	What happens
Any normal email address, e.g. `alice@yourcompany.com` or `it-alerts@yourcompany.com`	The message (a scan, report or alert) is sent as email from a designated mailbox in your tenant.
`<name>@sharepoint.local`, e.g. `accounting@sharepoint.local`	The attachment is converted to PDF (if it is not one already) and filed in the SharePoint folder mapped to `accounting`. Ideal for scanned documents.

Administrators manage the `@sharepoint.local` address book through a web page, choosing destination folders from a live view of the SharePoint site. No configuration files need editing to add a new destination, and changes take effect immediately.

What it works with

Printer scan-to-email and scan-to-SharePoint is the biggest use case, and the product is designed and marketed around it. But anything that sends email over SMTP is relayed the same way:

- **Multi-function printers and copiers** - scan to email, or straight into a

SharePoint folder.

- **UPS units** (APC, Eaton and others) - power, battery and self-test alerts.
- **Server management controllers** - HP iLO, Dell iDRAC, Lenovo XClarity

hardware and health alerts.

- **NAS devices** (Synology, QNAP and others) - job, disk and backup notices.
- **Phone systems, PBXs and VoIP** - voicemail-to-email and system alerts.
- **Alarm, access-control and building-management systems.**
- **Monitoring tools and line-of-business applications** that email reports.

The email-relay path serves all of these; the SharePoint-upload path is the document-centric extra that suits scanners. Devices that have no real mailbox of their own are covered by the fixed-sender option, so every alert arrives from one consistent, trusted address.

Key features

- **Drop-in for printers.** Unauthenticated SMTP on the LAN, no TLS required,

configurable port. The printer's settings change once and never again.

- **Scan to email via Graph.** Sent from the printer's own From address or,

more commonly, a single fixed scanner mailbox. Attachments of any size the mailbox accepts are supported, including those over Graph's inline limit.

- **Scan to SharePoint via Graph.** Direct upload into any folder of any

document library on the configured site, with automatic renaming on filename conflicts.

- **PDF conversion.** TIFF (including multi-page), JPEG, PNG, BMP and GIF

scans become a single multi-page PDF. Existing PDFs pass through untouched.

- **Never loses a scan.** Every message is written to disk before the printer

is told "accepted". Transient Microsoft outages or throttling are retried with exponential backoff; permanent failures are kept for an administrator to re-queue, and an alert email is sent.

- **Unmapped addresses are held, not dropped.** A scan to an address with no

folder yet is parked and the administrator alerted; once the folder is mapped, one click delivers it.

- **Web administration.** Routes with a folder picker, connection settings,

sender policy, a status page with job history, queue depths, token health, and a connection test. Single administrator account with bcrypt hashing, a forced password change on first login, CSRF protection and login throttling.

- **Least-privilege Microsoft 365 footprint.** The app identity has only

`Mail.Send` and `Sites.Selected`. An Exchange Application Access Policy limits sending to the scanner mailbox, and the SharePoint grant covers only the one site.

- **Operational hygiene.** Structured JSON logs rotated daily, systemd

services running as an unprivileged user with sandboxing, nftables rules restricting both ports to named subnets, and a one-shot PowerShell script that performs the entire Entra ID / Exchange setup.

Who it is for

Small and medium organisations on Microsoft 365 with one or more legacy devices or services that email scans, reports or alerts, and somewhere on the LAN to run the relay (a VM, an existing server, or a small appliance such as a Raspberry Pi). The system is designed to be installed by an IT generalist in an afternoon and then forgotten about.

What it is not

- Not a general-purpose open mail relay. It accepts mail only from your own

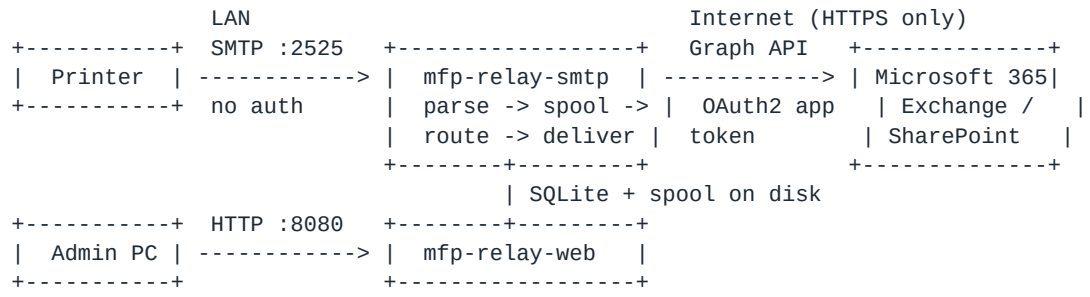
LAN devices and is never exposed to the internet; it exists to get their messages into Microsoft 365, not to forward arbitrary traffic.

- Not an OCR or document management system. Files are converted to PDF and

delivered; their content is not read.

- Not multi-tenant. One installation serves one Microsoft 365 tenant.

Architecture at a glance



Two independent systemd services share a SQLite database and an on-disk spool. A fault in the web interface cannot interrupt mail delivery, and vice versa.

Requirements

Component	Requirement
Server	Debian 12 or 13 (other systemd-based distributions should work), 1 vCPU, 1 GB RAM, a few GB of disk for the spool
Network	A LAN address reachable by the printers; outbound HTTPS to `login.microsoftonline.com` and `graph.microsoft.com`
Microsoft 365	Global Administrator access for the one-time setup; a mailbox (shared mailboxes are fine) to send scans from; a SharePoint site
Printers	Ability to send scans by SMTP to a custom host and port, with authentication and TLS disabled

Documentation set

Document	Audience	Contents
Installation Guide	Installer	Microsoft 365 setup, server installation, firewall, printer configuration, verification, upgrades
Administrator Manual	Day-to-day admin	Web interface, routes, settings, status page, CLI, logs, backups, credential rotation, troubleshooting
Technical Specification	Engineers	As-built architecture, message flow, routing rules, Graph integration, data model, configuration reference, security model, limits
Vendor Guide	Interop Solutions	Signing key, issuing licences, building images and updates, the setup app
Roadmap	Interop Solutions	Multi-platform plan and milestones (appliance, Linux, Raspberry Pi, Windows)

Document	Audience	Contents
Route to Market	Interop Solutions	What remains before selling and supporting the product
Original design spec	Reference	The design brief the product was built from

Licence

MIT. See `pyproject.toml`.