

Microsoft 365 SMTP AUTH: scan-to-email survival runbook

Draft 0.1, 18 October 2026. Not Microsoft software; not affiliated with or endorsed by Microsoft. Not legal, security or tenant-specific advice. Not tested on a real tenant or device. Evidence labels: **[V]** the author opened the cited page and it says this; **[P]** third-party write-up; **[A]** vendor claim; **[G]** guess.

1. What changes, and when [V]

Microsoft's post of Jan 27 2026 (<https://techcommunity.microsoft.com/blog/exchange/updated-exchange-online-smtp-auth-basic-authentication-deprecation-timeline/4489835>):

- Now to December 2026: SMTP AUTH Basic Authentication behavior remains unchanged.
- **End of December 2026: SMTP AUTH Basic Authentication will be disabled by default for existing tenants. Administrators will still be able to enable it if needed.**
- New tenants created after December 2026: SMTP AUTH Basic Authentication will be unavailable by default. OAuth will be the supported authentication method.
- Second half of 2027: Microsoft will announce the final removal date for SMTP AUTH Basic Authentication.

What this means: a device that logs in with a mailbox username and password to `smtp.office365.com` may stop sending at the end of December unless you (a) move it to a supported method, or (b) have an admin turn Basic back on as a **temporary** stopgap. Microsoft has not said when the stopgap ends. Check the live post before acting; Microsoft's own January 2026 post describes the update as giving customers "additional runway", i.e. the schedule has already been revised once. We could not find an exact December day [not verified].

2. Plan in one page

1. **Inventory** who sends with Basic auth (section 3).
2. **Classify** each sender: device or app? recipients internal only? OAuth supported? static IP or certificate available? (section 4)
3. **Pick a path** per sender (section 5).
4. **Implement** one sender at a time with a test and a rollback (sections 6 to 8).
5. **Stopgap** only for what cannot move in time (section 9). Write down an owner and a date.

3. Inventory

3.1 The admin center report [V]. New Exchange admin center > Reports > Mail flow > **SMTP AUTH clients**. Choose a range up to 90 days (default is 7 days; "If the report is empty, try changing the

date range"). Columns shown: Sender address, Domain, Authentication Protocol (Basic Auth = `TlsAuthLogin`, Modern Auth = `X0AUTH2`), TLS 1.0 / 1.1 / 1.2 (percentages), Messages sent. Click **Export** for a CSV. Source: <https://learn.microsoft.com/en-us/exchange/monitoring/mail-flow-reports/mfr-smtp-auth-clients-report>. Roles that can view: Compliance Administrator, Exchange Administrator, Organization Management, Security Administrator, Security Reader, View-Only Recipients.

Caution [not verified]: Microsoft's page lists the column labels but shows no sample CSV, so we do not know the exact header row of the exported file. The kit's analyzer is built to tolerate variations and tells you when it had to guess.

3.2 Per-message detail [P]. A third-party blog says the report page also has a "Request Report" option (hours to generate, emailed link) and lists its columns as `date`, `message_id`, `senderName`, `senderDomain`, `tls_version`, `tls_cipher`, `original_client_ip`, `authMethod`, `message_count`, with IP addresses concealed as "PII" unless a tenant reporting setting is changed (check your privacy policy first). This is **not** on Microsoft's page we read. The same blog gives a `Start-HistoricalSearch ... -ReportType SmtplibCSReport` command; Microsoft's `Start-HistoricalSearch` page does not list that report type, so treat it as unconfirmed. The analyzer accepts this layout and uses the IP column to help you find the device.

3.3 Read-only settings (PowerShell). Run `powershell/Get-SmtplibAuthInventory.ps1` yourself after `Connect-ExchangeOnline`. It only uses `Get-TransportConfig`, `Get-CASMailbox`, `Get-MailUser -HVEAccount`, `Get-InboundConnector`, and writes CSVs locally. **Untested on a real tenant.** Meaning of the values [V]: `SmtplibClientAuthenticationDisabled` True = off, False = on, blank on a mailbox = follow the org setting; the mailbox value wins. If **Security defaults** are on in Entra, SMTP AUTH is already disabled; if an **authentication policy** disables Basic for SMTP, clients cannot use SMTP AUTH even if you enable it (<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission>).

3.4 Run the analyzer (`app/index.html`, double-click; no install, no network). Paste or open the CSV. Optionally paste the posture/mailbox output. It lists senders still on Basic, flags TLS 1.0/1.1, and proposes fix paths you can refine with the drop-downs.

3.5 Physical hunt. The report names mailboxes, not devices. Match sender addresses to devices (ask the office, check each device's SMTP page, use the IP column if you have it).

4. Four questions per sender

Question	Why it matters
Printer/scanner, WordPress/site, or custom app?	Decides which guide applies
Any recipient outside your tenant?	High Volume Email is internal-only [V]
Does this exact model/firmware support OAuth 2.0 for Exchange Online?	OAuth is Microsoft's recommended method [V]; device lists are in the guides

Question	Why it matters
Static public IP or a TLS certificate available?	Needed for SMTP relay connector [V]

Also: does the device support TLS 1.2? Microsoft says client SMTP submission requires TLS 1.2 or 1.3 and port 465 defaults are unsupported [V].

5. Fix paths, with the facts that matter

Each row names the Microsoft Learn page it comes from. Short names: **Device page** = <https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365> ; **HVE page** = <https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/high-volume-mails-m365> ; **OAuth page** = <https://learn.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth> ; **Graph page** = <https://learn.microsoft.com/en-us/graph/api/user-sendmail?view=graph-rest-1.0> ; **SMTP AUTH page** = <https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission> .

Path	Use when	Facts [V, from the page named in brackets, unless marked]
OAuth on smtp.office365.com:587	Device/app supports it	Needs licensed mailbox + SMTP AUTH enabled for it; TLS 1.2/1.3; limits 10,000 recipients/day, 30 messages/minute [Device page]. Device-code sign-ins may need to be redone periodically (HP says so [A]).
High Volume Email	All recipients are inside your tenant	smtp.hve.mx.microsoft:587; no licence/mailbox ("Do not assign licenses to HVE accounts"; no mailbox, cannot receive email); pay-as-you-go at \$0.000042 per recipient and needs an Azure billing policy; 50 recipients/message; 10 MB; Worldwide cloud only; Basic or OAuth [HVE page].
SMTP relay + inbound connector	External recipients, no OAuth, device can use port 25	MX endpoint, port 25, certificate or static unshared IP; no Sent Items; not for third-party-hosted senders; add to SPF; "reasonable limits" [Device page].

Path	Use when	Facts [V, from the page named in brackets, unless marked]
Graph sendMail / SMTP XOAUTH2 client credentials	Software you control	Mail.Send and "202 Accepted... doesn't indicate that the request processing has completed" [Graph page]; client-credentials SMTP needs SMTP.SendAsApp, New-ServicePrincipal, mailbox FullAccess grant [OAuth page].
Third-party sending service	No OAuth and no static IP/cert, or hosted apps mailing customers	Not evaluated here; needs DNS (SPF/DKIM) and an account; cost varies [G].
Your own mail server as relay	You already run one	Microsoft lists this option; says Windows Server 2022 is the last version with the IIS SMTP feature and that it is unsupported for relaying to Microsoft 365 [Device page].
Non-email scan destinations	Scan-to-folder is enough	SMB/FTP etc. (vendor-suggested [A]).
Stopgap: re-enable Basic	Cannot move in time	Admins "will still be able to enable it"; final removal date unannounced; blocked by Security Defaults [SMTP AUTH page; timeline post].
Avoid: Direct Send as a long-term answer: anonymous mail to your own tenant's recipients only, and Microsoft says "We're working on an option to disable Direct Send by default" [V: Device page]. Avoid new Azure Communication Services Email builds: Microsoft announced on Sep 23 2026 that ACS Email retires Sep 30 2028 and limits onboarding from Oct 23 2026 for customers without an ACS resource created before that date; the same page says new ACS Email resources can currently still be created, "subject to change at any time" [V: https://learn.microsoft.com/en-us/azure/communication-services/acs-retirement-and-breaking-changes-guide]. The Device page still lists ACS Email as an option; weigh the retirement.		

6. Implementing, per path (summaries; full steps in [guides/](#))

OAuth device: update firmware to the vendor's OAuth release; configure in the device's admin UI; sign in with the sending mailbox; confirm Authenticated SMTP is enabled for it; send a test; record when the sign-in expires. **HVE:** create the HVE account (Exchange admin center > Mail flow > High Volume Email); attach a billing policy; point the device at `smtp.hve.mx.microsoft:587` with TLS; set Reply-To; test an internal address. **Relay connector:** create inbound connector (Your organization's email server > Office 365); authenticate by certificate subject (recommended) or the public IP; device to MX endpoint:25 with TLS; SPF; test internal and external. **Graph/XOAUTH2 app:** Entra app registration; permission; admin consent; (for SMTP) `New-ServicePrincipal` with the Enterprise-app object ID, `Add-MailboxPermission`; token scope `https://outlook.office365.com/.default`; restrict the app's reach [G].

7. Test plan (every sender)

1. Send to an internal and an external address (HVE: internal only).
2. Check the From address and, if it differs from the sign-in account, Send As (error 5.7.60 "Client doesn't have permissions to send as this sender" means missing permission [V: Device page]).
3. Check the message landed in Inbox, not Junk (SPF for relay) .
4. Re-run the SMTP AUTH clients report a day later: the sender should show Modern Auth or disappear from the Basic list.
5. Check the device's own SMTP log.

8. Rollback

Keep the old settings written down. Until the default flips, Basic keeps working as today [V]. After it flips, rollback means the stopgap (section 9). Do cutovers during business hours with someone at the device.

9. The stopgap, done carefully

Re-enabling Basic auth lowers your security: Microsoft says Basic "makes it easier for attackers to capture user credentials" [V: <https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>]. Treat it as a short, owned exception.

- **Prefer per mailbox**, not org-wide: `Set-CASMailbox -Identity <mailbox> -SmtpClientAuthenticationDisabled $false` (the mailbox setting overrides the org setting) [V: SMTP AUTH page].
- **Test:** send from the device, then run `Get-CASMailbox -Identity <mailbox> | Format-List SmtpClientAuthenticationDisabled` and confirm `False`; re-run the SMTP AUTH clients report next day.

- **Rollback (undo the exception):** `Set-CASMailbox -Identity <mailbox> -SmtpClientAuthenticationDisabled $null` (follow the org setting) or `$true` (disable) [V: SMTP AUTH page].
- **Org-wide is a bigger step** and affects every mailbox that follows the org setting: `Set-TransportConfig -SmtpClientAuthenticationDisabled $false` to enable; undo with `... $true`; verify with `Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled` [V: SMTP AUTH page]. Write down the current value first.
- **Security defaults** must be off for Basic SMTP to work [V: SMTP AUTH page]. Turning them off changes your tenant's wider security posture (they cover more than SMTP), so decide that with whoever owns your identity security; do not do it just for a printer.
- Record: owner, reason, date to remove. Microsoft will announce a final removal date in H2 2027 [V]; put a calendar check on the Microsoft post.
- Use a dedicated mailbox with a long unique password; do not reuse a person's mailbox [G].

10. Common traps

- Device "From" differs from the sign-in mailbox (needs Send As) [V].
- Port 465 configured [V]. Use 587.
- Old firmware that only does TLS 1.0/1.1: Microsoft states the TLS 1.2/1.3 requirement for client submission [Device page, V]; that old firmware is the usual cause is [G]. Some vendors note cipher changes (Ricoh [A]).
- HVE chosen for a sender that mails customers (internal-only) [V].
- HVE account has no mailbox and cannot receive email; Microsoft says to configure a Reply-To so replies reach a real mailbox [V: HVE page].
- OAuth set up once; the device-code sign-in expires and scanning silently stops (HP says its setting expires at regular intervals [A]).
- A mailbox with `SmtpClientAuthenticationDisabled = $true` overrides the org setting [V: SMTP AUTH page]; HP's OAuth instructions say to check that Authenticated SMTP is enabled for the mailbox [A: HP support page; not re-fetched on 18 Oct, its server returned HTTP 500], so expect OAuth to fail too until it is enabled [I].
- Security defaults or an authentication policy blocking Basic regardless of your setting [V].

11. What this kit does not do

It does not log in to your tenant, change settings, send mail, or contact Microsoft. It does not evaluate third-party relay vendors. It has not been run on a real export. No PowerShell command (including the ones in section 9 and the inventory script), device, or tenant has been tested. The report-CSV header row is unverified (section 3). Everything dated is as fetched on 18 Oct 2026.

12. Sources

See `sources/EVIDENCE.md` for quotes and links. Key links: - Timeline:

<https://techcommunity.microsoft.com/blog/exchange/updated-exchange-online-smtp-auth-basic-authentication-deprecation-timeline/4489835> - SMTP AUTH clients report:

<https://learn.microsoft.com/en-us/exchange/monitoring/mail-flow-reports/mfr-smtp-auth-clients-report> - Device/app sending options: <https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365> - Enable/disable SMTP AUTH: <https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission> - High Volume Email:

<https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/high-volume-mails-m365> - OAuth for SMTP: <https://learn.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth> - Graph sendMail:

<https://learn.microsoft.com/en-us/graph/api/user-sendmail?view=graph-rest-1.0> - ACS retirement:

<https://learn.microsoft.com/en-us/azure/communication-services/acs-retirement-and-breaking-changes-guide>