



DOCUMENT WORKFLOWS | SPECIAL REPORT

SPECIAL REPORT

Your Copier May Stop Scanning to Email in 2026

What Microsoft 365 authentication changes mean for multifunction printers and scanners

A practical readiness guide for South African SMEs that rely on scan-to-email—and do not want an authentication change to become an office emergency.

AUGUST 2026 • EDUCATIONAL BUSINESS TECHNOLOGY REPORT

EXECUTIVE SUMMARY

Executive Summary

A multifunction printer can keep copying and printing normally while its scan-to-email function fails. The reason may have nothing to do with the scanner mechanism. It may be the way the device signs in to Microsoft 365.

Microsoft is phasing out Basic Authentication for SMTP AUTH in Exchange Online. Under its January 2026 timetable, behaviour remains unchanged through December 2026. At the end of December 2026, Basic Authentication will be disabled by default for existing tenants, although administrators will still be able to re-enable it temporarily if needed. Microsoft plans to announce the final removal date in the second half of 2027.

Devices that send mail using a stored username and password may need supported firmware, OAuth 2.0 configuration, newer TLS security and changes inside Microsoft 365. Some older models may not support the required combination at all.

The central management message: Do not wait for scan-to-email to fail. Identify every device and workflow that sends mail through Microsoft 365, confirm how it authenticates, test the approved replacement configuration and record who owns ongoing support.

A sensible readiness review should answer five questions:

- Which printers, scanners, applications and other devices send email through the organisation's Microsoft 365 environment?
- Is each device using Basic Authentication, OAuth 2.0, SMTP relay or another approved method?
- Does the exact model and installed firmware support both OAuth 2.0 and Microsoft's required TLS cipher suites?
- Who can change the device, Microsoft 365 and network settings—and who will test the result?
- What alternative workflow will staff use if a device cannot be upgraded?

MAIN ARTICLE

Your Copier May Stop Scanning to Email in 2026

The office copier may be working perfectly. Its connection to Microsoft 365 may not be.

Picture a Monday morning in a busy office. A signed contract is placed in the document feeder, the employee selects a saved email address and presses Start. The pages scan. Then the machine reports an authentication or transmission error. Printing still works. Copying still works. The address book is still there. Yet the document does not leave the machine.

This is the type of failure Microsoft's security changes can expose. It is not unique to one copier brand, and it is not solved merely by changing the email password.

1 What is actually changing?

Many printers, scanners and business applications send email through Exchange Online using SMTP AUTH. With Basic Authentication, the device commonly presents a mailbox username and password. Microsoft regards this as an outdated security method because a stolen password can be reused and the sign-in does not provide the protections available through token-based Modern Authentication.

Microsoft's preferred direction is OAuth 2.0, where access is authorised through a token rather than repeatedly presenting the account password. Tokens can be limited to a particular application or resource and have a limited usable lifetime.

The timing needs to be stated carefully. Microsoft updated the deprecation schedule on 27 January 2026. According to current guidance, SMTP AUTH Basic Authentication behaviour remains unchanged through December 2026. At the end of December 2026, it will be disabled by default for existing tenants, but administrators will still be able to re-enable it temporarily if required. For new tenants created after December 2026, it will be unavailable by default and OAuth will be the supported authentication method. Microsoft plans to announce the final removal date in the second half of 2027.

This is not a claim that every copier will stop on the same day. It is a warning that a device still dependent on Basic Authentication has a known compatibility risk that should be resolved while there is time to test it.

2 Why a copier can print but no longer email

Printing, copying, scanning and emailing are separate parts of the workflow. A device may scan the paper correctly but fail when it tries to connect to the outgoing mail service. That failure can occur at several points:

Point in the chain	What may be wrong	Typical evidence
Device firmware	The model has no OAuth 2.0 support, or the required firmware has never installed.	Vendor model list, firmware version and release notes
Authentication	The device still uses a stored username and password through Basic Authentication.	Device email settings and Microsoft 365 sign-in or SMTP reports
Encryption	The device does not support the TLS version or cipher suites required by Microsoft 365.	Vendor compatibility notice and connection logs
Microsoft 365	SMTP AUTH, mailbox permissions or the approved application authorisation is not configured correctly.	Tenant and mailbox configuration
Network and naming	DNS, firewall rules, port settings, certificate validation or time settings prevent a secure connection.	Network test, device log and error code

This separation is important when troubleshooting. Replacing toner, cleaning the scanner glass or rebooting the copier may have no effect on an authentication failure.

3 OAuth support is necessary—but may not be sufficient

A supplier may confirm that a model supports OAuth 2.0. That is encouraging, but it is not the end of the check. Product-specific technical guidance shows that some devices need a firmware update before OAuth

2.0 can be configured, after which the authentication settings must still be completed through the device's management interface.

Published compatibility guidance also shows that OAuth 2.0 support alone may not be enough. A device must support the encryption standards required by Microsoft 365; otherwise, it may still be unable to connect to Exchange Online.

The same principle applies across brands: test the exact model, controller, firmware and configuration. A general statement that "this range supports Microsoft 365" is not the same as evidence that the installed machine is ready.

Readiness requires a working combination: compatible hardware + supported firmware + modern authentication + supported encryption + correct Microsoft 365 settings + a successful end-to-end test.

4 Which office functions may be affected?

Scan-to-email is the most visible example, but manufacturers identify other email-dependent functions that may use the same route:

- Sending scanned documents by email
- Internet fax or fax-to-email forwarding
- Automatic device-status and error notifications
- On-demand email notifications
- Mail-to-print or related email-driven workflows where supported

The review should therefore cover the complete device workflow, not only the button employees use most often. It should also include other equipment and applications that send email with stored Microsoft 365 credentials, such as alarm panels, monitoring systems, line-of-business software and older servers.

5 Do not solve a security change by weakening security

When a legacy device cannot sign in, the quickest workaround can look attractive: create another account, remove controls, use a password that never changes or expose a less secure relay. That can restore a message while creating a larger security and governance problem.

Any replacement method should be approved by the organisation's Microsoft 365 administrator or competent support provider. Microsoft documents several ways for devices and applications to send mail. The appropriate choice depends on whether recipients are internal or external, the device's capabilities, the organisation's tenant and security policies, message volumes and the level of administration available.

Possible route	When it may fit	Questions that must be resolved
OAuth 2.0 through SMTP AUTH	The device and firmware support modern authentication and the required encryption.	Who authorises the device, maintains firmware and re-tests after changes?
Microsoft 365 SMTP relay	A controlled relay design suits the organisation and its network.	Are connectors, certificates or fixed public IP requirements understood and secured?
Direct Send	A limited internal-recipient use case fits Microsoft's rules.	Will mail need to reach external recipients, and how will delivery and abuse risk be controlled?
Approved third-party relay or workflow	The device cannot meet Microsoft 365 requirements directly.	Where is data processed, what is logged, what does it cost and who supports it?
Scan to folder or document platform	Email is not essential and a controlled document workflow is preferable.	Can staff access it easily, are permissions correct and is the process backed up?

These are decision routes, not universal recommendations. The solution must be designed for the organisation's environment and tested without bypassing security controls.

6 An illustrative South African SME example

Consider a 35-person professional-services business with two multifunction printers. Both use the same Microsoft 365 mailbox to send signed documents and supplier invoices. One newer machine supports OAuth 2.0 after a firmware update. The older machine does not appear on the manufacturer's supported list.

A useful response is not to replace both devices immediately. The business can update and configure the newer machine, test internal and external recipients, confirm PDF attachment delivery and record the settings. For the older machine, it can evaluate a controlled relay, scan-to-folder workflow or planned replacement based on cost, remaining contract term and operational importance.

A potentially costly outcome is discovering the problem during a tender submission, month-end process, customer onboarding or compliance deadline—then paying for an emergency workaround without time to assess the risk.

7 What to ask your equipment and Microsoft 365 providers

Responsibility is frequently split. The copier provider understands the model and firmware; the Microsoft 365 provider controls the tenant and mailbox; the network provider controls firewalls, DNS and routing; the internal manager owns the business process. If nobody coordinates the whole chain, each supplier may correctly say that its own component is working while the scan still fails.

- What is the exact model, controller and current firmware version?
- Does this configuration support OAuth 2.0 for Exchange Online SMTP submission?
- Does it support Microsoft's required TLS version and cipher suites?
- Is a firmware update available, and could that update affect any existing settings or applications?
- Which Microsoft 365 mailbox, application registration, connector or relay method is used?
- Can the proposed method send to both internal and external recipients where required?
- Who will perform and document the end-to-end test?
- What is the fallback if the installed model cannot be made compliant?

8 Test the business workflow, not only the connection

A technician may prove that the copier can send one message to an internal address. That does not necessarily prove that the normal business workflow is ready. The acceptance test should reflect actual use.

Test	Evidence to retain
Send a one-page PDF internally	Received message, correct sender, timestamp and readable attachment
Send a multi-page PDF externally	Delivery beyond the tenant, attachment size and image quality
Use address-book and manual recipients	Both approved methods work without exposing unnecessary addresses
Test colour, duplex and higher-resolution scans	File size, processing time and delivery remain acceptable
Restart the device and repeat the test	Authentication survives normal reboot and reconnection
Trigger an approved device notification	Status or error email reaches the responsible person
Review logs and failure escalation	Support can identify the device, error and responsible provider

Where the workflow handles personal, confidential or commercially sensitive documents, confirm the sender mailbox, access permissions, audit records, retention and any third-party processing. Authentication readiness is part of information security, not merely copier maintenance.

PRACTICAL TOOL

Scan-to-Email Readiness Record

Complete one line for every multifunction printer, scanner, application or device that sends email.

The record is designed to prevent a vague assurance such as “Microsoft 365 is configured.” Every important conclusion should be supported by a model list, configuration record or successful test.

Decision area	Required answer or evidence	Status / owner
Device identity	Brand, exact model, serial number, location and business owner	Pass / Gap / N/A
Workflow	What is sent, how often, internal/external recipients and business deadline	Pass / Gap / N/A
Current method	Basic Auth, OAuth 2.0, relay, Direct Send, third-party service or unknown	Pass / Gap / N/A
Firmware	Installed version and vendor-supported target version	Pass / Gap / N/A
OAuth support	Written evidence for the exact model and firmware	Pass / Gap / N/A
TLS support	Evidence that Microsoft 365 encryption requirements are supported	Pass / Gap / N/A
Microsoft 365 setup	Mailbox, permissions, app/connector and administrator responsible	Pass / Gap / N/A
Network path	DNS, ports, firewall, certificates, time settings and fixed-IP dependencies	Pass / Gap / N/A
Internal test	Date, recipient, result and retained evidence	Pass / Gap / N/A
External test	Date, recipient, result and retained evidence	Pass / Gap / N/A
Fallback	Approved alternative if the device cannot send email	Pass / Gap / N/A
Next review	Review date, trigger events and named owner	Pass / Gap / N/A

Acceptance rule: Mark the workflow ready only when the exact installed device has passed the required internal and external tests using the approved authentication route, and the result, owner and fallback have been recorded.

CLOSING PERSPECTIVE

Treat scan-to-email as a managed business workflow

For many SMEs, scan-to-email became part of the office years ago and then disappeared from management attention. It works, so nobody asks how it works. Microsoft's authentication changes are a useful reminder that the copier is connected to the same identity, network and cloud environment as other business systems.

The answer is not panic or automatic replacement. It is an inventory, a compatibility check and a controlled test. Newer equipment may need only firmware and configuration. Older equipment may require a different sending method, an alternative document workflow or a planned replacement. The right decision depends on the business process, the security requirements and the remaining value of the device.

The practical question is simple: if Microsoft 365 refused the copier's current sign-in tomorrow, would your team know which machines are affected, who owns the fix and how documents would still move? If the answer is no, the readiness review should begin before the error message appears.

Important note: *This report is educational and reflects published Microsoft and manufacturer guidance available in August 2026. Microsoft's enforcement timetable, product firmware and supported methods may change. Configuration must be confirmed for the organisation's specific Microsoft 365 tenant, device model, firmware and security requirements.*