LOFFLER

> **December 2026 -** **Microsoft announced they are deprecating SMTP AUTH. This guide will go over what this change means and how it will affect scanning with MFPs in a business environment, and outlines replacement options such as unauthenticated mail relay and configuring OAuth 2.0 for outbound mail. Refer to Microsoft's official deprecation timeline for the most current information.**

> **Note**: As of January 28, 2026, this guide reflects the latest available information. Microsoft has not announced a final, universal cutoff date for all Basic Authentication scenarios. Always verify current status and timelines using the official Microsoft documentation.

What is SMTP AUTH?

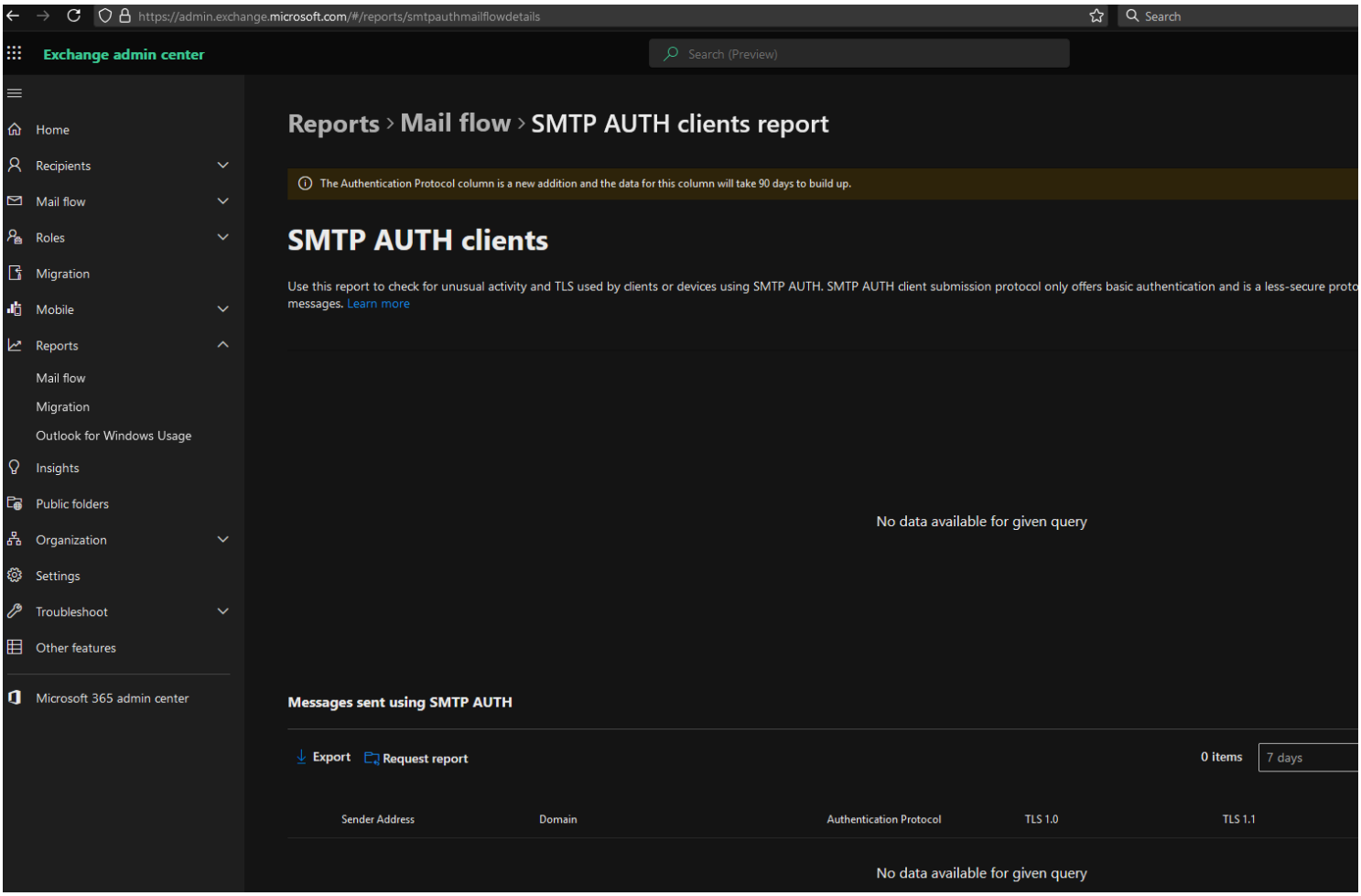
SMTP AUTH is a process that allows only authorized users to send email to an SMTP server. It's a mechanism built into the SMTP protocol that requires the user to authenticate before sending messages, in this context, it would be the MFP emailing scanned documents (PDFs) via SMTP. The MFP connects to the SMTP server, provides the credentials (username and password), the server checks the credentials against its database of authorized users. If authentication is successful, the SMTP server allows the email to be sent. If authentication fails, the server rejects the request.

Why Does SMTP AUTH Matter to Me?

Many companies use SMTP AUTH to authenticate to their email server, which allows the MFP to send scanned documents to email destinations.

Am I Affected by This Change?

Companies that use BASIC AUTH with Microsoft Exchange Online to send email from an MFP are affected by this change. Review the SMTP settings on your MFP, to see how it's configured. Microsoft offering a report to find out if your company is affected https://admin.exchange.microsoft.com/#/reports/smtpauthmailflowdetails



- **SMTP Server** is Microsoft-based, such as:
  - `smtp-mail.outlook.com`
  - `mail.protection.outlook.com`
  - `smtp.office365.com`
  - `smtp-legacy.office365.com`
- **SMTP Authentication** is enabled.

- **Username and Password** are entered for SMTP authentication.

Additionally, you may check your Entra ID activity logs. If you have MFPs authenticating using Basic AUTH, that activity will be listed there.

- Log into the Azure Administration Portal (**portal.azure.com**)
- Click **Microsoft Entra ID**
- Expand "**Monitoring**", and select "**Sign-in logs**", review for some things listed below:
  - **Authentication requirement**: Basic Authentication
  - **Display Name**: MFP Printer Name
  - **Authentication method**: Basic
  - **Protocol**: SMTP
  - **IP Address**: Compare against your list of MFPs

If these factors are present, your configuration will be impacted by Microsoft's changes.

How Will This Affect MFP Scan-to-Email?

After Basic Authentication is disabled, devices configured to use this login method will no longer be able to authenticate and send emails, causing the scan job to fail.

Available Options in Place of SMTP AUTH

There are some options to address this change to SMTP AUTH. Here is an overview of each option, the details are provided further in this guide.

- **Option 1: Upgrade to a more secure solution -** We offer solutions that eliminate the need for SMTP altogether: www.loffler.com/office-copiers
    - UniFlow, Papercut, Ysoft, etc. centrally managed.
    - Manufacturer Cloud based applications
- **Option 2: SMTP Relay through Office 365 - Microsoft Solution:**
    - This option requires no authentication at the MFP level and is secured through TLS and IP based authentication. Once the relay is configured, the same configuration is used on each MFP.
- **Option 3: O-Auth 2.0 Based Authentication- MFP Manufacturer Solution:**
    - OAuth 2.0 based authentication set on each individual MFP – This option requires a compatible MFP (not all MFPs support OAuth 2.0) and is configured on each MFP individually, not centrally managed.
- **Option 4: Azure Communication Services Email - Microsoft Solution:**
    - Microsoft Azure Communication Services Email scalable, enable businesses to build engaging business-to-consumer (B2C) experiences. Integrates with Azure monitoring, credentials often long (ensure device supports long passwords), and is configured on each MFP individually, not centrally managed.
- **Option 5: High Volume Email for Microsoft 365 - Microsoft Solution:**
    - Microsoft High Volume Email (HVE) is a Microsoft-managed service designed to send large volumes of automated, outbound email from applications, MFP without relying on traditional Exchange Online mailboxes. This option is for internal email only, configured on each MFP individually, also not centrally managed.
- **Option 6: Third-Party SMTP or Email Provider - Other Solution:**
    - Third-party email service providers can be used as an alternative to Microsoft 365 for scan-to-email and application-based email delivery. Many providers support standard SMTP authentication (username and password), while others offer API key–based authentication or both. The same configuration may also used on each MFP.

Option 1: Upgrade to a more Secure Solution

In some cases, SMTP authentication and OAuth 2.0 are not required. Loffler offers solutions that simplify communication without setting up an email relay or adjusting any SMTP settings in your environment. Such as Uniflow, Papercut, YSoft and other manufacturers cloud-based services. We invite you to speak with your sales representative for more details on these options.

Secure Document Scanning & Printing Services | Loffler

Option 2: Microsoft Unauthenticated Mail Relay (Recommended)

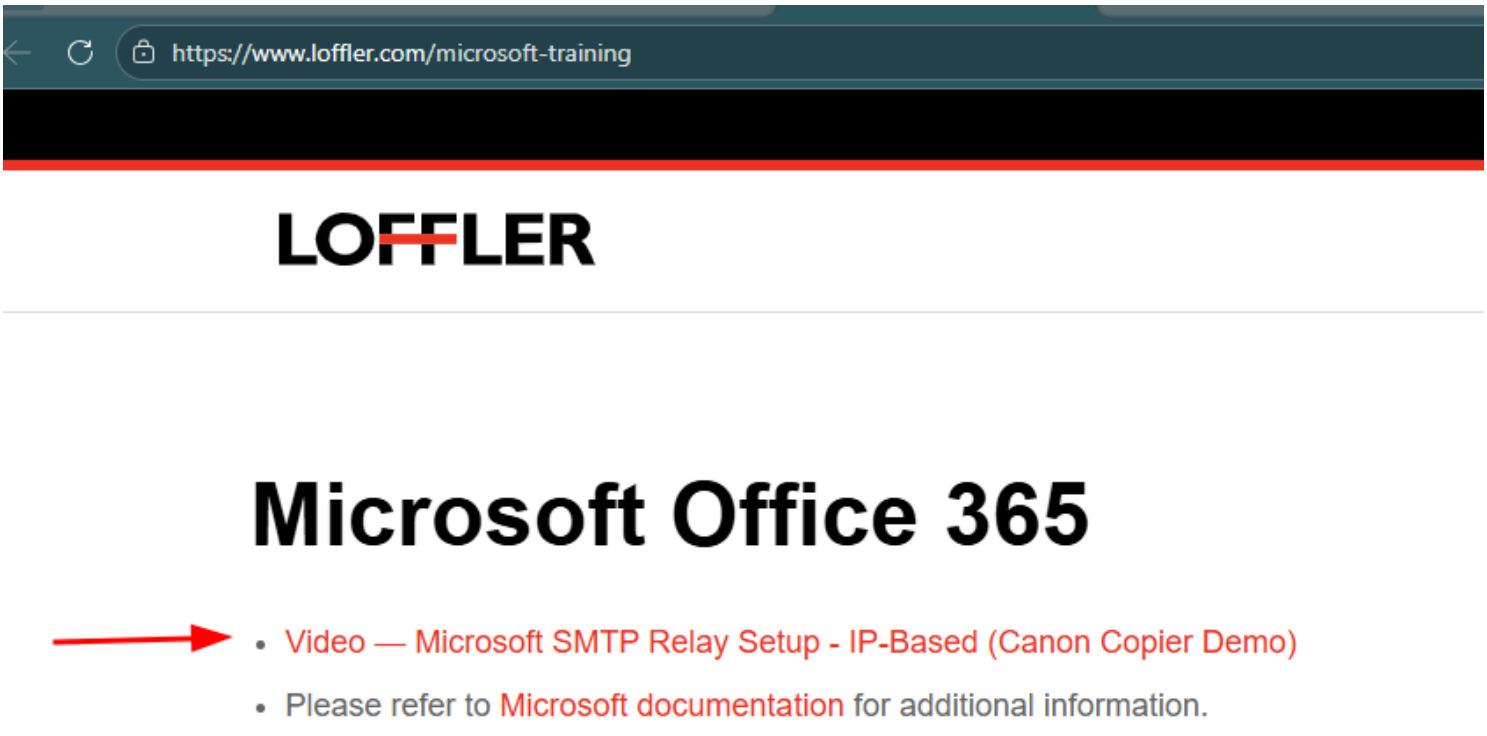
Things to know about Unauthenticated Mail Relay:

- **Note on Security:** Although this method is listed as “unauthenticated”, (means you’re using an allowed IP address instead of username and password) it remains secure because the relay is restricted to approved IP addresses, preventing unauthorized use. Messages are only accepted from trusted internal sources, and TLS encryption is used, to ensure that emails remain protected in transit.
- **DNS Edit:** Require login to the domain name registrar for DNS records edit.
- **Functions**: Using an unauthenticated relay can allow MFPs to continue to use scan-to-email functions when Microsoft removes the ability to use basic authentication when connecting to Office 365.
- **Connector & Mail Flow:** The application or device in your organization's network uses a connector for SMTP relay to send emails to recipients in your organization.
- **Security & Authentication:** The Microsoft 365 or Office 365 connector you configure authenticates your device or application with Microsoft 365 or Office 365 using an IP address.
- **Mailbox & Licensing**: Microsoft 365 or Office 365 SMTP relay doesn't require the use of a licensed Microsoft 365 or Office 365 mailbox to send emails.
- **IP Address reputation:** Sent mail can be disrupted if your IP addresses are blocked by a spam list.
- **Public Address Requirement:** Requires static unshared external IP addresses, multiple public IP address for sending email are supported.

Microsoft Resources: How to set up a multifunction device or application to send email using Microsoft 365 or Office 365 | Microsoft Learn

Loffler Setup Video Direct Link: Microsoft SMTP Relay Setup

Also available at Loffler training page:



Note: The video uses a Canon copier to demonstrate, but the email relay information may be implemented with any copier.

Option 3: OAuth 2.0

Open Authorization 2.0 (OAuth 2.0) provides modern authentication protocols, offering enhanced security by eliminating the need to store usernames and passwords directly on the devices. Each manufacturer offers specific instructions for enabling OAuth 2.0 on their devices, if available. Below you'll find a brief overview for some of the more common brands, along with links to more detailed technical documentation, if available.

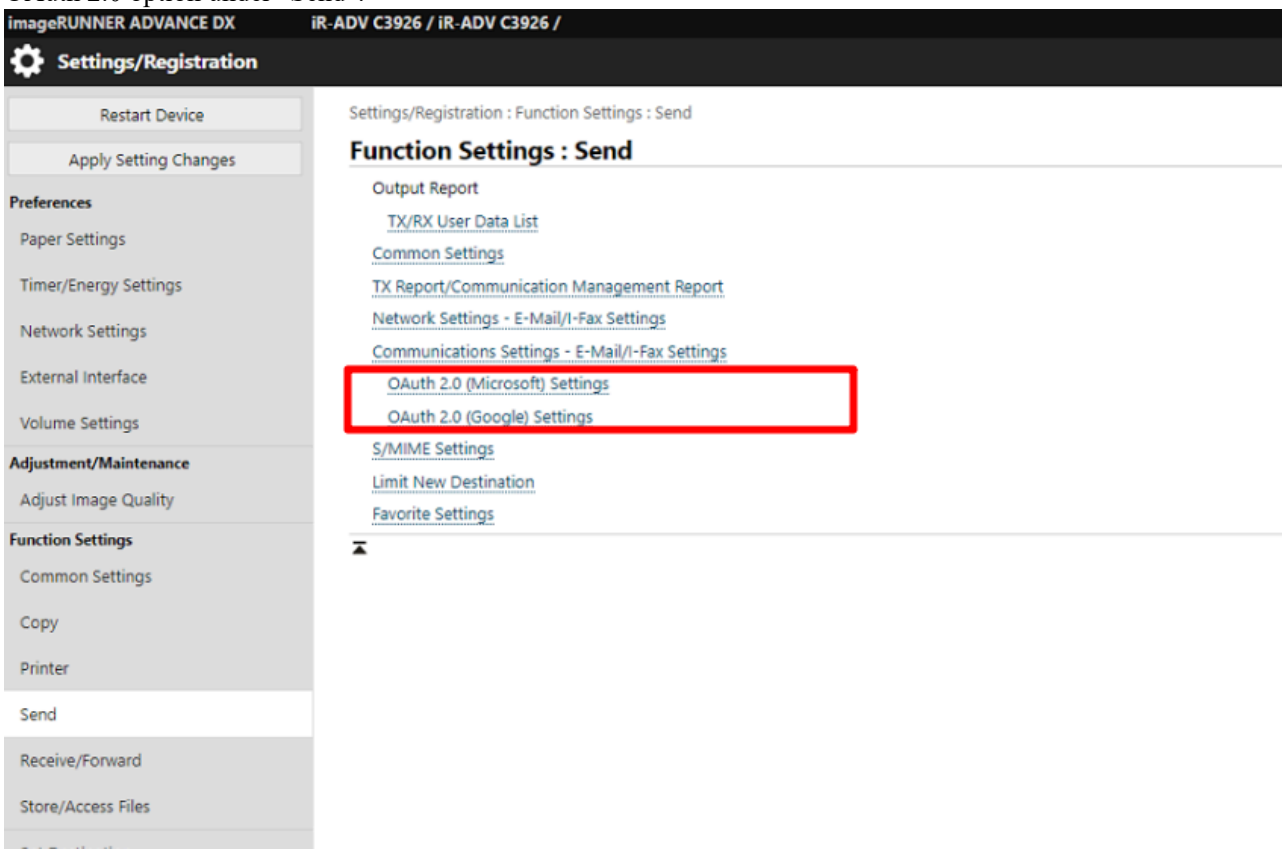
General guidelines for setting up OAuth 2.0:

- **Account & Licensing Requirements:** Configuration of OAuth 2.0 authentication requires a licensed mailbox/account in the O365 tenant. This account will be used as the sender for email sent from the MFP.
- **Credential:** Ensure you have the credentials for the licensed account.
- **Tenant & Identity Configuration:** The licensed account must have Modern Authentication enabled in the O365 admin center.
- **Alternative Account Option:** If not using an O365 tenant and/or no licensed mailbox/account is available, create a Microsoft Outlook account for this purpose here: **https://signup.live.com**.

OAuth 2.0 setup guide by the MFP Manufacturer:

- **Canon MFP**: Canon MFP must be on unified Firmware Platform (uFP) v3.18 or higher. For more firmware support information, please contact Loffler imaging helpdesk. If the devices is supported, you will able to see the

OAuth 2.0 option under "Send":



- Canon Online Manual Resource: Link .
- Loffler Setup Videos:
  - Video 1 - Scan-to-Email OAuth 2.0 Set up and Troubleshoot with O365 and GoDaddy Account
  - Video 2 - Scan-to-Email OAuth 2.0 with Google Account (Alternative to the Google APP Password)

- **HP MFP**: To use OAuth 2.0 on HP MFPs, please be sure to upgrade your firmware to HP FutureSmart 5.7 or newer, HP Oauth2.0 Setup Guide: HP Setting Up Scan To Email OAuth v2.0 Authentication (HP PDF).
- **Konica-Minolta MFP:** Konica-Minolta has limited support for OAuth 2.0 using a supported firmware is needed, Officials supported documentation: OAuth2.0 support notice for SMTP authentication (KM PDF).
- **Lexmark MFP**: Lexmark printers support OAuth 2.0 authentication starting with the FW24 firmware. For more support view Lexmark instructions here (Lexmark Website) .
- **Xerox MFP**: Currently Xerox support modern authentication like OAuth 2.0 are also limited, supported model and instructions: Configuring Scan to Email Using OAuth 2.0 (Xerox Website). An unauthenticated relay (Option 1 above) is recommended for other unsupported Xerox MFPs.

Option 4: Azure Communication Services Email

Azure Communication Services (ACS) can be used to send transactional and operational email from devices and applications. ACS is a paid, pay-as-you-go service (metered per message, per recipient, and features) and is a good option if you want cloud-native, scalable email that integrates with Azure identity and monitoring.

Things to know:

- **Paid service**: ACS is billed through your Azure subscription (pay-as-you-go). Consult your Azure billing admin for pricing and quota details.
- **Authentication**: ACS supports API keys/connection strings and modern auth patterns rather than traditional username/password. When an SMTP credential is issued it may be a long token/API key.
- **Long password/API key support**: Many ACS credentials are long. Ensure the copier/MFP supports long credentials.
- **Deliverability**: You'll need to publish CNAME, SPF, DKIM (if the provider supports it) and monitor bounce reports. ACS supports domain verification and sending from custom domains.
- **Rate limits & throttling**: ACS imposes throughput limits — review the service quotas for high volume needs.
- **DNS Edit**: Require login to the domain name registrar for DNS records edit.

Microsoft Resource: Overview of Azure Communication Services email - An Azure Communication Services concept article | Microsoft Learn

Loffler Setup Video: Azure Communication Services Email SMTP Setup with Scan-To-Email - Canon Copier Demo

---

Option 5: High Volume Email for Microsoft 365

Microsoft's **High Volume Email (HVE) for Microsoft 365** is a cloud email capability designed to let organizations send **very large amounts of email primarily to internal recipients** without the standard recipient rate limits of regular Exchange Online mailboxes. HVE began its **public preview in April 2024** and has been evolving through enhancements such as **support for OAuth (modern authentication)** in addition to Basic Authentication, improved administrative setup in the Exchange admin center, and expanded domain support. Its **general availability (GA)** has been **moved to March 2026** to ensure a stable and fully supported release. Initially, the public preview included limits on the number of HVE accounts and daily recipient counts, but those **recipient rate limits have since been removed** and account limits increased, simplifying adoption during preview. HVE is focused on **internal tenant email**, with **external sending being removed** to clarify its role in the Microsoft 365 ecosystem; for external high-volume or transactional email scenarios, Microsoft recommends using **Azure Communication Services (ACS)** for email instead. Throughout the preview, Basic Authentication will continue to be supported **through September 2028**, though Microsoft encourages planning for OAuth to take advantage of stronger security.

Additional Things to know:

- **Public preview timeline:** HVE public preview started April 1, 2024 for a free experience, with general availability now targeted for **March 2026, pricing structure may applies.**

Microsoft Resource 1: Public Preview: High Volume Email for Microsoft 365 | Microsoft Community Hub

Microsoft Resource 2: Updates to High Volume Email (HVE) Public Preview | Microsoft Community Hub

Microsoft Resource 3: High Volume Email: Continued support for Basic Authentication & other important updates | Microsoft Community Hub

Loffler Setup Video: High Volume Email Microsoft 365 Quick Video

---

Option 6: Third-Party SMTP or Email Provider

Third-party SMTP or email service providers may be used as an alternative to Microsoft 365 or Azure-based solutions. Many providers support basic SMTP authentication (username and password) as well as API-based authentication, depending on the service. This option may be suitable when Microsoft-based solutions are not available or when a specific third-party service better fits operational or IT requirements.

> ⚠ **Important**: Microsoft and third-party email server configuration is customer-managed. Loffler supports copier-side configuration only. Customers without managed IT services should contact their internal IT team or IT provider for server-side setup and changes.
