

Configuring FileWave Server Mail Preferences

What

FileWave Server Mail Preferences controls outgoing email used for scheduled reports and other FileWave-generated messages. FileWave Central 16.4 provides two authentication methods under Preferences > Mail: Manual Setup for an SMTP server or relay, and OAuth for Google or Microsoft 365.



Version boundary: Manual SMTP configuration has been available in FileWave for many releases. OAuth mail authentication was introduced in FileWave 16.1.1. FileWave 16.4 fixes an issue where Username and Password could be required even when the SMTP server did not require authentication.

Choose an authentication method

Method	Use it when	Required configuration
Manual Setup	The organization uses an SMTP relay, transactional-mail service, app password, or other direct SMTP configuration.	Host, port, TLS choice, sender address, and credentials only when the SMTP server requires them.
OAuth	Google or Microsoft 365 is the mail provider and organization policy permits a provider application to send mail.	Provider application, FileWave callback URL, client information, provider authorization, and a valid token.

FileWave may generate a large volume of mail when scheduled reports or notifications are used broadly. Confirm the provider's sending limits and whether a transactional-mail service or dedicated relay is more appropriate than a personal mailbox.

Manual Setup

1. In FileWave Central, open Preferences > Mail.
2. Set Authentication Method to Manual Setup.
3. Enter the SMTP Host and Port supplied by the mail administrator or provider. The value initially displayed by Central is not a substitute for the provider's documented port.
4. Select Use TLS when required by the provider.
5. Enter Username and Password when the SMTP server requires authentication. When the relay intentionally permits the FileWave Server to send without SMTP authentication, leave both fields empty. FileWave 16.4 corrects prior validation that could incorrectly require those fields.
6. Enter the Send from (email address) value permitted by the mail system.
7. Choose Send test mail and confirm that the message reaches the destination and is not rejected or quarantined.

FileWave Central Admin Preferences

General Organization Info Mobile Google LDAP Kiosk VPP & ADE Inventory Mail Education Imaging Editor Proxies Software Upd < >

Mail Setup

Authentication Method: Manual Setup

Host:

Port: 25

☐ Use TLS

Username:

Password:

Send from (email address):

 No email has been sent using this account yet

Keep in mind that the email server needs to possibly handle thousands of emails (e.g. [Postmark](#) or [MailChimp](#)).

Send test mail



Do not use a normal account password when the provider requires an app password or OAuth. For Google Manual Setup, see the related [Google app-password troubleshooting](#) article below.

OAuth

OAuth avoids storing a normal mailbox password in FileWave. Before selecting Authorize, create a provider application and configure this exact FileWave callback pattern as a Web redirect URI:

```
https://<filewave-server-fqdn>:20445/inv/notifications/configuration/auth-callback
```

Replace `<filewave-server-fqdn>` with the fully qualified domain name users and the provider can resolve for the FileWave Server. The scheme, port, and callback path must match the redirect URI registered with the provider.

Complete OAuth in FileWave Central

1. Open Preferences > Mail and set Authentication Method to OAuth.
2. Select Google or Microsoft 365.
3. Enter the provider application's Client ID and Client Secret. Microsoft 365 also requires the Tenant ID.
4. Choose Authorize and complete the provider sign-in and consent process using the mailbox that FileWave should use.
5. Return to FileWave Central and confirm that the status shows Token Available.
6. Choose Send test mail and verify delivery.

FileWave Central Admin Preferences

General Organization Info Mobile Google LDAP Kiosk VPP & ADE Inventory Mail Education Imaging Editor Proxies Software Upd < >

Mail Setup

Authentication Method: OAuth

Provider: ☐ Google ☒ Microsoft 365

Client ID: REDACTED

Client Secret:

Tenant ID: REDACTED

☒ Token Available
☐ No email has been sent using this account yet

Keep in mind that the email server needs to possibly handle thousands of emails (e.g. [Postmark](#) or [MailChimp](#)).

Send test mail Authorize

Microsoft 365

1. Open the [Microsoft Entra admin center](#) and create an App registration.
2. Add the FileWave callback URL above as a Web redirect URI.
3. Copy the application's Client ID and directory Tenant ID.
4. Create a client secret and record its value securely when Microsoft displays it.
5. Ensure the account used during authorization has an Exchange Online license and is permitted to send mail under the organization's policy.
6. Enter the Client ID, Client Secret, and Tenant ID in FileWave Central, then select Authorize.



Record the client-secret expiration date. Rotate the secret in Entra and reauthorize FileWave before it expires.

Google

1. Open the [Google Cloud Console](#) and create or select a project dedicated to FileWave mail.
2. Configure the Google Auth Platform for that project. Select the audience required by the organization; Internal is commonly appropriate for a single Google Workspace tenant.
3. Create an OAuth client with Web application as the application type.
4. Add the FileWave callback URL above under Authorized redirect URIs. An Authorized JavaScript origin is not required for this FileWave workflow.
5. Enable the Gmail API for the same project.
6. Copy the Client ID and Client Secret into FileWave Central, then select Authorize.

Verify and monitor mail

- Test immediately: A saved configuration is not proven until Send test mail succeeds and the message is received.
- Review status: OAuth should show Token Available. Manual Setup and OAuth also show whether mail has been sent successfully through the configured account.
- Exercise the real workflow: Send a scheduled report to a controlled recipient after the basic test passes.

- Monitor provider limits: Review rate limits, sender restrictions, spam handling, and mailbox or relay quotas.
- Protect credentials: Keep Client IDs, Tenant IDs, client secrets, SMTP credentials, and authorized mailbox details out of screenshots and unapproved support notes.

Troubleshooting

Symptom	Check
Send test mail is unavailable or fails	Confirm required fields, provider host and port, TLS choice, DNS, firewall access, sender authorization, and provider quotas.
SMTP relay does not require authentication	Leave Username and Password empty and verify that the relay permits the FileWave Server's address to send. FileWave 16.4 includes a correction for prior validation that could incorrectly require those fields.
OAuth authorization fails	Compare the registered Web redirect URI with the FileWave callback URL exactly, then verify provider application status, consent, license, API availability, Client ID, Tenant ID when applicable, and client secret.
Token is unavailable or later stops working	Reauthorize the provider and check whether the client secret, provider consent, mailbox license, or organization policy changed.
Google Manual Setup returns Bad Request	Use OAuth when appropriate, or verify Google 2-Step Verification and an app password for the Manual Setup workflow.

Related content

- [Google SMTP Manual Setup: Bad Request and App Passwords](#)
- [Generating Scheduled Reports](#)
- [Sending Scheduled Reports to More Than One Address](#)
- [FileWave Central Preferences](#)

🔄Revision #3

★Created 2026-07-12 00:40:23 UTC by Josh Levitsky

✎Updated 2026-07-12 00:47:55 UTC by Josh Levitsky