AP 3-Way Match

User Manual - Internal Staff Edition (Admin / Approver / Viewer)

A complete, screenshot-illustrated guide to every screen and workflow. Personal and Server editions share this exact same manual.

12 October 2026

Table of Contents

Getting Started 4

- What this app actually does, in plain terms . . . 4
- Signing in . . . 4
- The shared layout . . . 5
- What the Dashboard shows . . . 5
- First-time setup checklist (for whoever's setting this up) . . . 6
- Purchase Orders — where they come from . . . 6

Admin Guide 8

- Managing users . . . 8
- Managing vendors . . . 9
- Audit Log . . . 11

Approver Guide 13

- Getting an invoice in . . . 13
- Reviewing what the AI read . . . 14
- The Review Queue (Gmail invoices needing a second look) . . . 17
- The Processed Queue . . . 18
- Transferring to your backend . . . 19
- Fraud detection you can't turn off . . . 19

Viewer Guide 21

- What's different about your sidebar . . . 21
- The Processed Queue — read, not act . . . 21
- Dashboard and PO Ledger . . . 22
- Settings — visible, but nothing saves . . . 22

Settings Reference 25

- Company Profile . . . 25
- Workspace tab . . . 27

My Account tab 34

AI Provider & Local Model Setup **35**

The three hosted providers 35

Getting your first API key 35

Custom (OpenAI-compatible) — for a local or self-hosted model 36

What switching providers does — and doesn't — do 37

Single Sign-On Setup **39**

What this actually does 39

Before you start: get the Redirect URI from this app 39

Part 1: Google 40

Part 2: Microsoft 42

How sign-in actually behaves 43

Troubleshooting 43

Keeping this secure 44

Getting Started

<- Back to Table of Contents

This chapter covers what's true for every role: signing in, the shared layout, and a first-time setup checklist for whoever's setting the system up.

What this app actually does, in plain terms

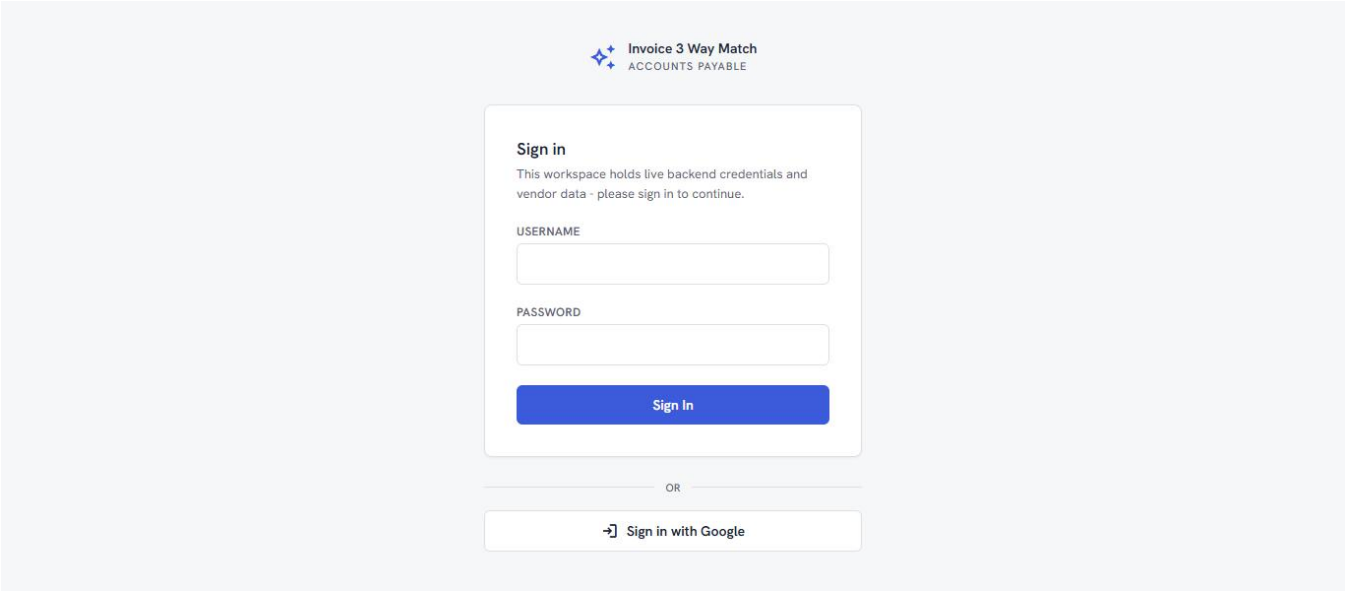
Before a supplier's invoice gets paid, three documents should agree with each other:

- **The Purchase Order (PO)** — what you actually ordered, and the price you agreed to.
- **The Goods Received Note (GRN)** — what you actually received (not always the same quantity as ordered — a partial delivery, for example).
- **The Invoice** — what the vendor is now billing you for.

"3-way matching" just means checking all three agree before money goes out — catching the ordinary mistakes (a wrong quantity, a price that crept up since the PO was raised) as well as the deliberate ones (a vendor billing twice for the same delivery, or quietly changing their bank details). This app reads an invoice, compares it against the other two automatically, and either confirms it's clean or flags exactly what doesn't line up — instead of someone manually checking three documents by eye, invoice after invoice.

Signing in

Open the address your admin gave you (e.g. `http://your-server:5000`) in a browser. You'll see the sign-in screen:



Sign in screen

Enter the username and password your admin created for you, and select **Sign In**.

> **Do:** bookmark this page so you don't have to ask for the address again.
> **Don't:** share your password with a colleague, even temporarily — if they need access, ask your admin to create them their own account (see the Admin Guide).

If your company has turned on **Single Sign-On**, you'll also see a **"Sign in with Google"** (or Microsoft) button below the form — see Single Sign-On Setup if your admin wants to turn this on. Using it signs you in with your existing company Google/Microsoft account instead of a separate password.

Vendors: if you're a supplier submitting invoices to this company rather than someone on their internal team, you don't use this screen at all — you have your own separate login. See the Vendor Portal Guide.

The shared layout

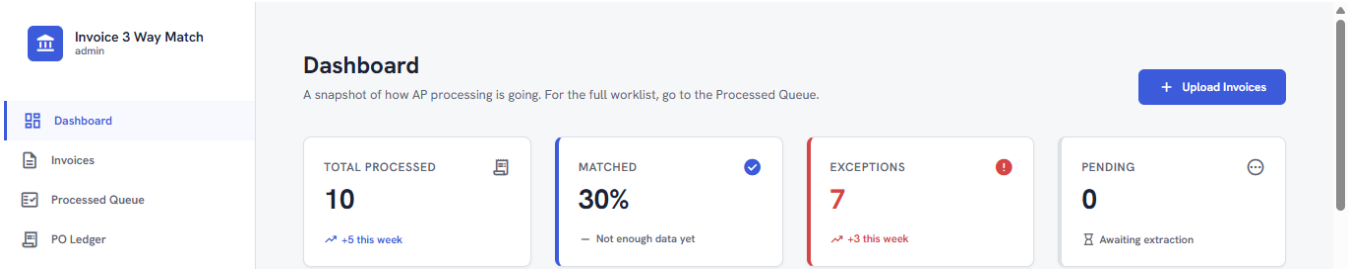
Once signed in, every screen shares the same left-hand sidebar. What appears in it depends on your role — see each role's own chapter for the full breakdown — but the overall shape is the same for everyone:

- Your company name and your own username appear at the top.
- Below that, links to every screen your role can reach.
- **User Guide**, near the bottom, opens this exact manual inside the app itself — worth bookmarking instead of asking a colleague every time.
- **Logout** is always the last item.

The very first screen you land on, every role alike, is the **Dashboard** — a glance-view of how AP processing is going. From there, **Invoice Ingestion** (Admins and Approvers only) is where new invoices get pasted, uploaded, or pulled in from email.

What the Dashboard shows

The Dashboard is a glance-view of how AP processing is going — not a worklist (that's the Processed Queue, covered in the Approver Guide).



Dashboard KPI tiles

- **Total Processed** — every invoice that's gone through extraction, ever.
- **Matched** — the percentage that reconciled cleanly against a purchase order.
- **Exceptions** — invoices that didn't reconcile and need a person to look at them.
- **Pending** — invoices mid-extraction (should normally read 0; a stuck number here for a

while is worth mentioning to your admin).

Below the tiles (not shown above) are a status-mix chart, your top vendors by invoice volume, and a "Needs Attention" list of the oldest unresolved exceptions.

First-time setup checklist (for whoever's setting this up)

If you're standing this system up for the first time, do these in order. If nobody has actually installed the application anywhere yet — there's no address to open, nothing to log into — start with Installation & Deployment instead; it covers everything before this checklist, with no technical background assumed.

1. **Log in** with the very first admin credentials — if you used the Windows one-click

installer, that's the email and temporary password shown on its Finish page (see Installation & Deployment); if you set this app up manually, it's the `APP_USERNAME`/`APP_PASSWORD` you chose in your `.env` file (see Installation & Deployment).

2. **Set your Company Profile** — Settings -> Company Profile. See

Settings Reference.

3. **Choose where your Purchase Order data comes from** — Settings -> Workspace -> Backend

Connection. If you don't have a live ERP/accounting system to connect, **Excel/CSV Import** is the zero-setup option: you upload a spreadsheet of open POs instead. See Settings Reference for every option.

4. **Choose an AI provider** to actually read your invoices — see

AI Provider & Local Model Setup. Nothing can be extracted from an invoice until this is configured.

5. **Create accounts for your team** — Users page, one per person, with the right role. See

the Admin Guide.

6. **Upload your open Purchase Orders** (if using Excel/CSV Import) — see

Purchase Orders, below.

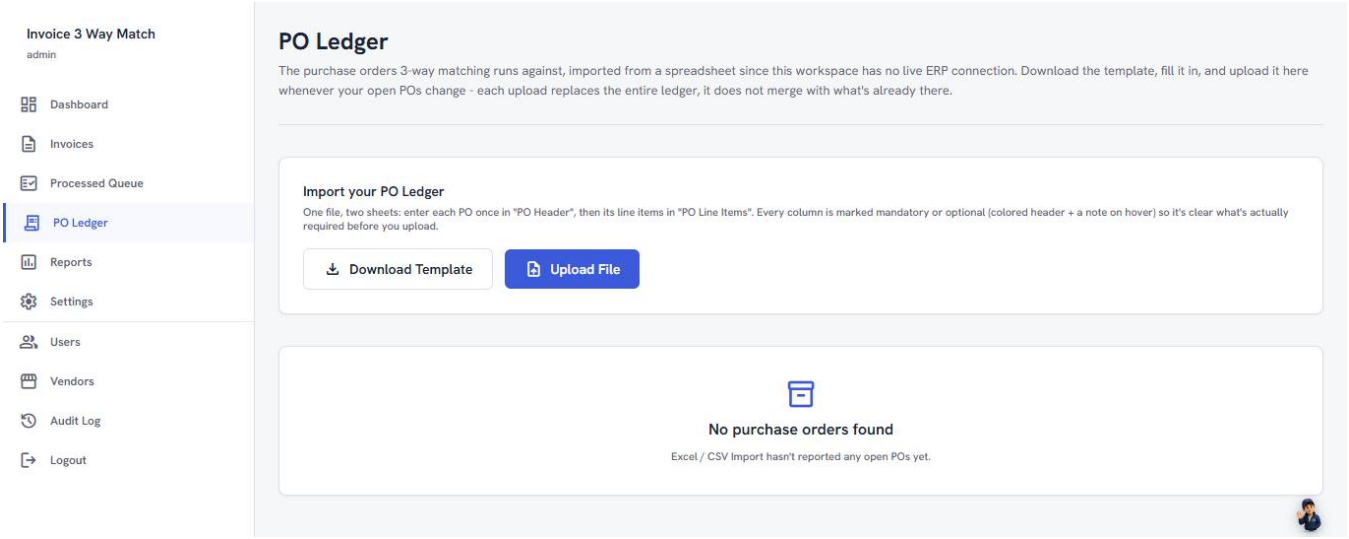
7. Optionally, set up **vendors** who'll submit their own tax/bank details through a

self-service portal — see Vendor Portal Guide, and **Single Sign-On** if your team already uses Google Workspace or Microsoft 365 — see Single Sign-On Setup.

Once that's done, you're ready to start ingesting real invoices — head to your own role's chapter: Admin, Approver, or Viewer.

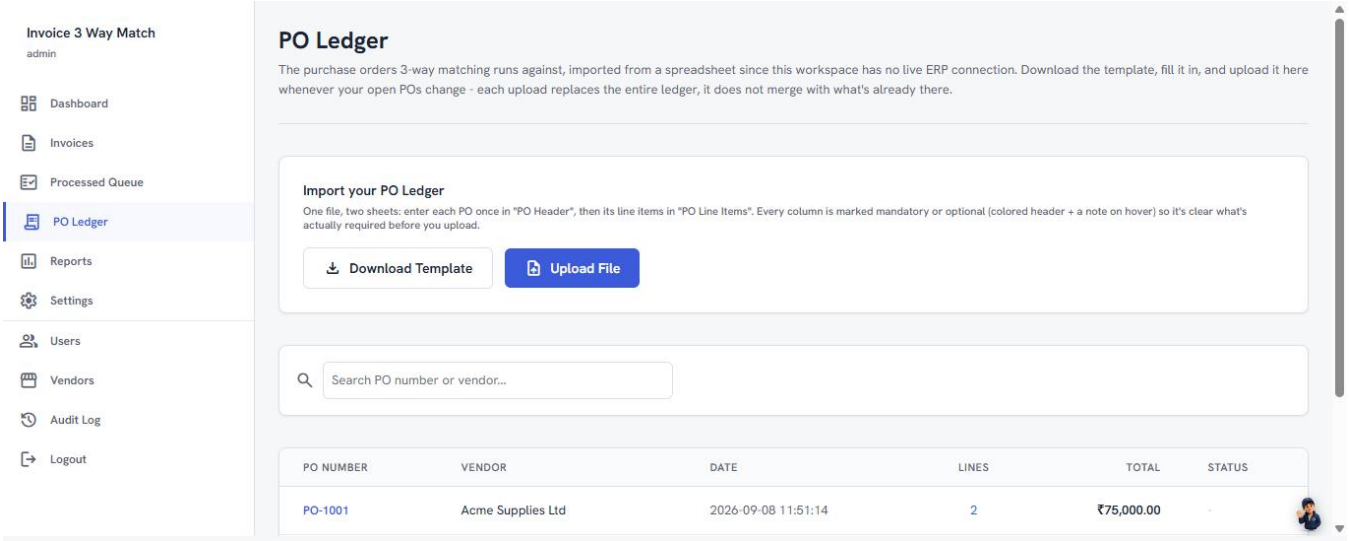
Purchase Orders — where they come from

Before you ingest your first real invoice, there needs to be something for it to match against. If you're using Excel/CSV Import (the no-ERP option), that starts out empty:



PO Ledger, empty state

Download the template, fill in your open purchase orders, and upload it (see Settings Reference for exactly how). Once uploaded, the PO Ledger shows what your 3-way matching will actually run against:



PO Ledger, populated

> **Do:** re-upload the file every time your open POs change — each upload **replaces** the whole ledger, it doesn't merge with what's already there.
> **Don't:** assume an invoice will match just because the vendor name looks right — the PO Number on the invoice has to match a PO Number in this ledger exactly.

Admin Guide

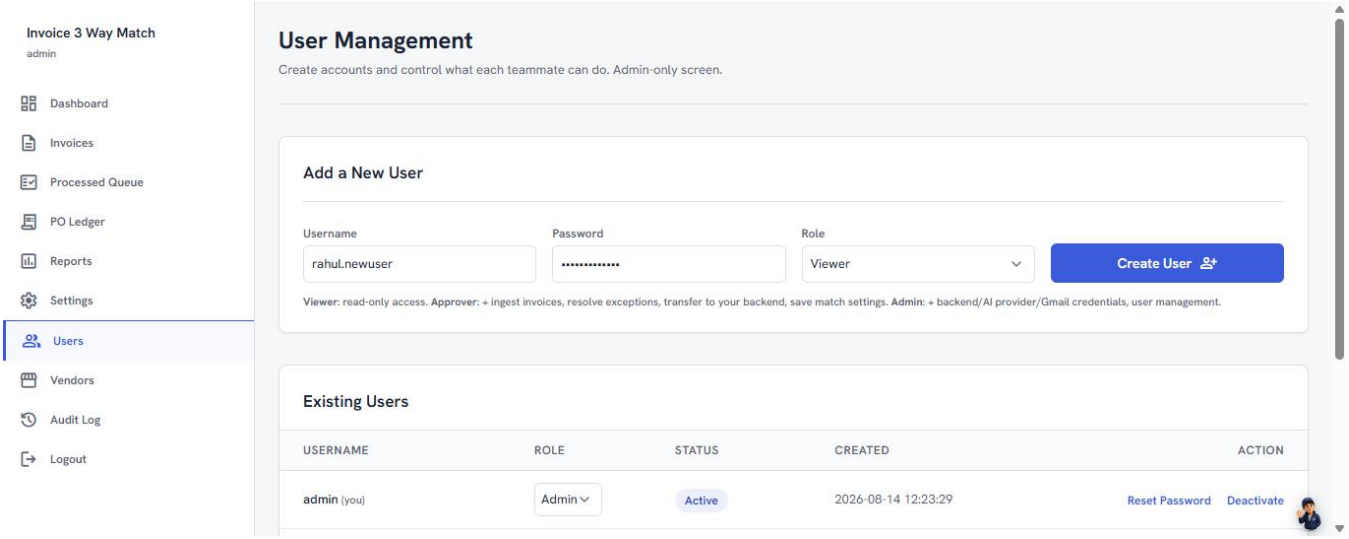
<- Back to Table of Contents

Admins have every capability Approvers and Viewers have, **plus** the screens covered here. If you're looking for how to ingest invoices, resolve exceptions, or read the Processed Queue, that's covered once, in the Approver Guide, since the day-to-day workflow is identical for Admins and Approvers.

This chapter covers what's **admin-only**: managing users, vendors, the audit trail, and your license. For every Settings screen in detail, see the Settings Reference — this chapter only covers Users, Vendors, and Audit Log, which live outside Settings.

Managing users

Users (sidebar) is where you create an account for every person on your team and control what they can do.



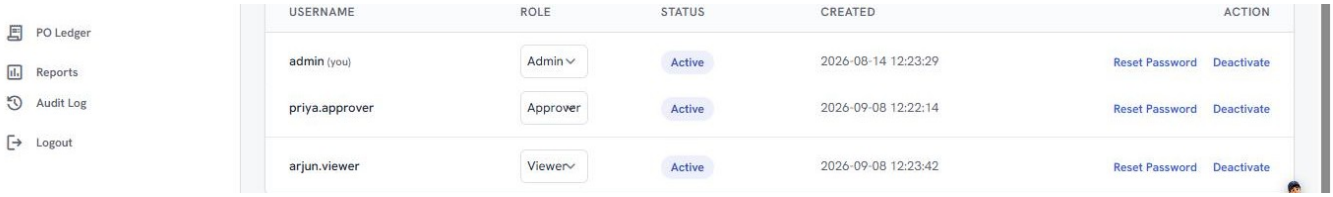
Add a New User form

Fill in a username, a temporary password (they can change it later from their own **My Account** settings), and pick a role:

- **Viewer** — read-only access everywhere.
- **Approver** — + ingest invoices, resolve exceptions, transfer to your backend, change match rules/tolerances.
- **Admin** — + everything in this chapter.

> **Do:** give each person their own account, even if two people share a desk. Every action is attributed by username in the Audit Log — sharing an account destroys that trail.
> **Don't:** create more accounts than your license allows — see **Licensing and seats** below.

The existing-users table lets you change anyone's role, reset their password, deactivate them, or (once already deactivated) delete them permanently:



Users list

A few rules worth knowing:

• **You can't deactivate or demote yourself**, and the system won't let the **last active

admin** be deactivated or demoted either — there always has to be at least one admin who can undo a mistake.

• **Resetting a password** immediately invalidates the old one. If that person's username

looks like a real email address, the new temporary password is **emailed to them automatically** — no review step, since you already explicitly triggered the reset, so there's nothing left for you to check before it reaches the one person it's for. If their username isn't email-shaped (or the email couldn't be sent), it's shown to you once instead — copy it before closing the dialog, since it isn't shown again, and relay it to that person yourself.

• **Deleting** a user is permanent and only available once they're already deactivated — a

deliberate two-step safety measure. Their past actions stay fully visible in the Audit Log either way; deleting the account doesn't erase their history.

Licensing and seats

Every **active** internal user (any role) counts against your license's seat count — vendor portal accounts never do. If you're at your limit, creating a new user shows:

> *"Your license allows 3 seats and all are in use. Deactivate an existing user or upgrade your license to add more."*

Deactivate someone who's left, or apply a license with more seats, from **Settings -> Company Profile -> License**. See Settings Reference for how to apply one.

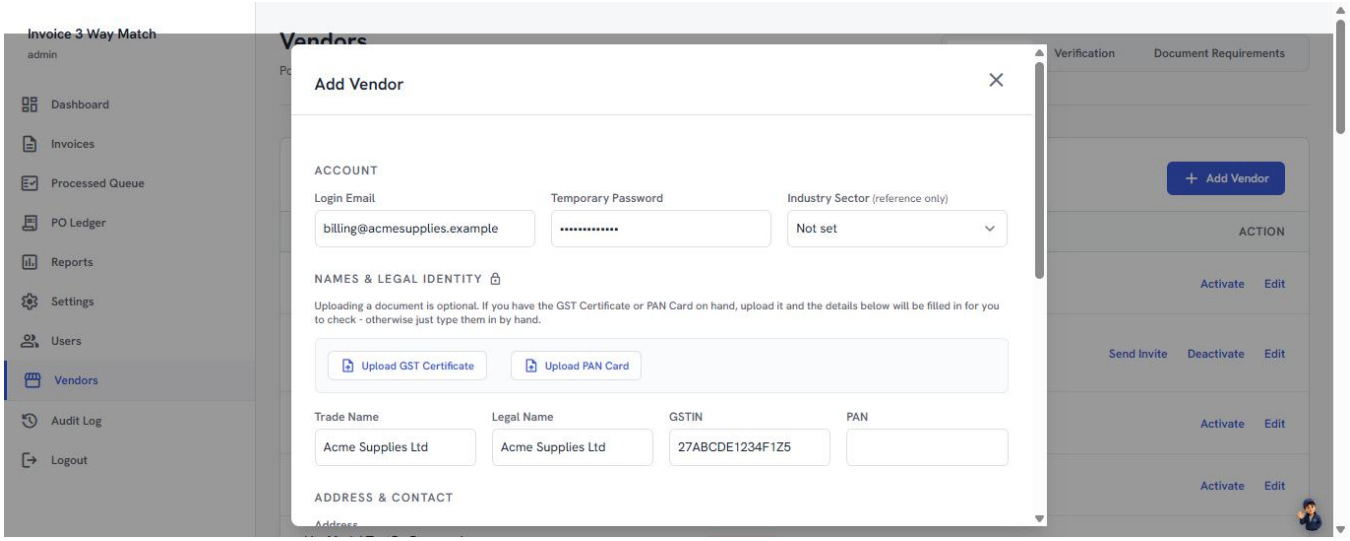
Already over your seat count (most often right after a trial ends, since the trial itself has no seat limit) works differently — you get a **10-day grace period** with nothing blocked, not an immediate lockout. See Settings Reference for exactly what that looks like and what happens once it runs out.

Managing vendors

Vendors (sidebar) has three tabs, all admin-only.

Accounts

Every vendor who can log into their own self-service portal (see the Vendor Portal Guide) is created here, the same way you create an internal user:



Add Vendor form

Trade Name, Legal Name, GSTIN, and PAN can be typed in by hand, or filled in automatically by uploading the vendor's GST Certificate or PAN Card — the app reads the document and you just confirm it's correct. Bank details work the same way with a cancelled cheque.

Once created, the vendor appears in your accounts list:



Vendor account row

- **Send Invite** drafts an email (in *your own* connected Gmail's Drafts folder — see

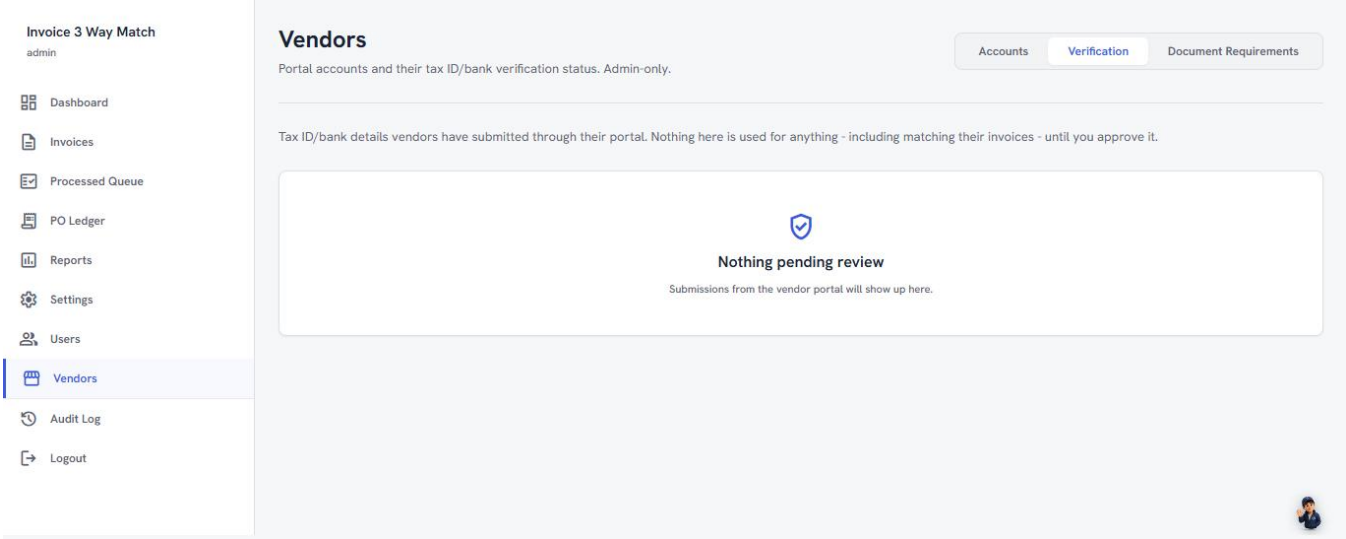
Settings Reference) with their login link and temporary password. It's a **draft**, not an auto-sent email — you review and send it yourself. Use this again any time later for a vendor created earlier, or if they've lost their password (it issues a fresh temporary one each time you send it). That login link is built automatically from whatever address you're reached at right now — see Installation & Deployment -> Find the address to open it at if you're ever unsure what that address actually is or why it might change.

- **Deactivate** blocks their portal login without deleting their data.
- **Edit** lets you correct any field.

> **Don't** assume a vendor's tax ID or bank details are trustworthy just because they typed something into their profile — see **Verification** below. Nothing they submit is used for fraud-checking until you approve it.

Verification

Whatever a vendor submits through their own portal (tax ID, bank account) lands here for your review — it's never trusted automatically:



Verification queue, empty

When a vendor does submit something, you'll see it listed with **Approve** and **Reject** options. Approving is what actually makes that tax ID/bank account count toward the fraud checks run against every invoice from that vendor (see the Approver Guide for what those checks catch). Rejecting requires a reason, which the vendor sees on their own side so they know what to fix and resubmit.

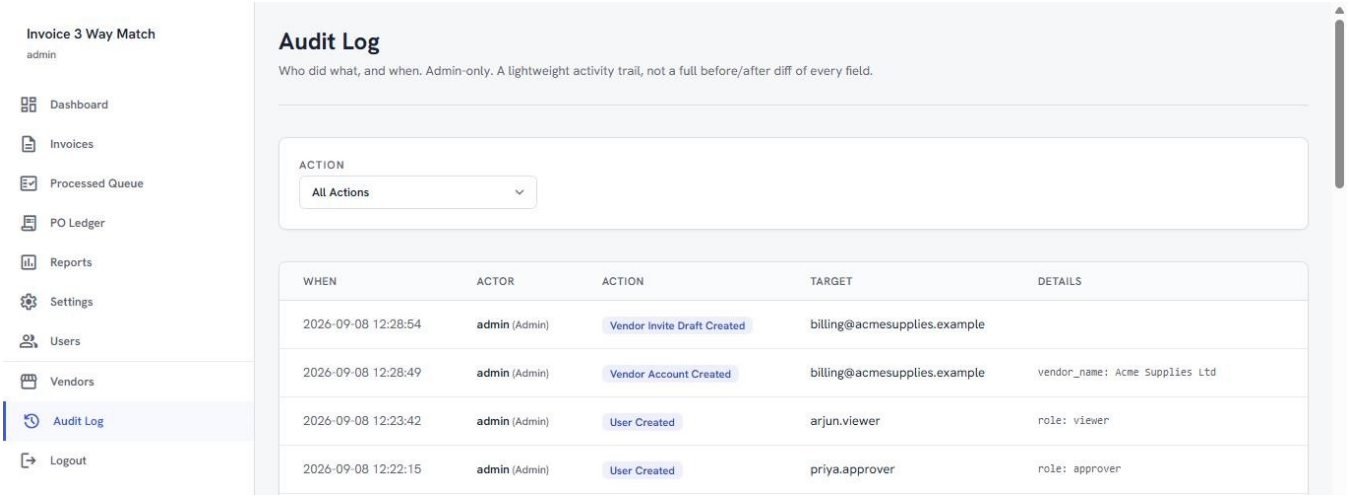
> **Do:** actually check a GST Certificate or cancelled cheque before approving — this queue exists specifically so a fraudster can't just type in a different bank account and have it silently accepted.

Document Requirements

Configure which documents every vendor is asked to submit, based on your own company's **Industry Sector** (set in Company Profile — see Settings Reference) and each vendor's own sector. A universal set (cheque, GST, PAN, Udyam) applies to every vendor regardless of industry.

Audit Log

A complete, filterable trail of who did what and when — every login (including failed attempts), every setting change, every invoice action, every user/vendor change:



Audit Log

Filter by action type using the dropdown at the top. This is a lightweight activity trail — it records *that* something happened and its key details, not a full before/after diff of every field that changed.

> **Do:** check here first if something looks wrong ("why is this invoice marked Approved?", "who changed the match tolerance?") — it's almost always faster than asking around.

Where to go next

- Day-to-day invoice processing (ingestion, exceptions, transfers): Approver Guide
- Every Settings screen explained: Settings Reference
- Choosing and configuring what reads your invoices: AI Provider & Local Model Setup
- Optional company login via Google/Microsoft: Single Sign-On Setup

Approver Guide

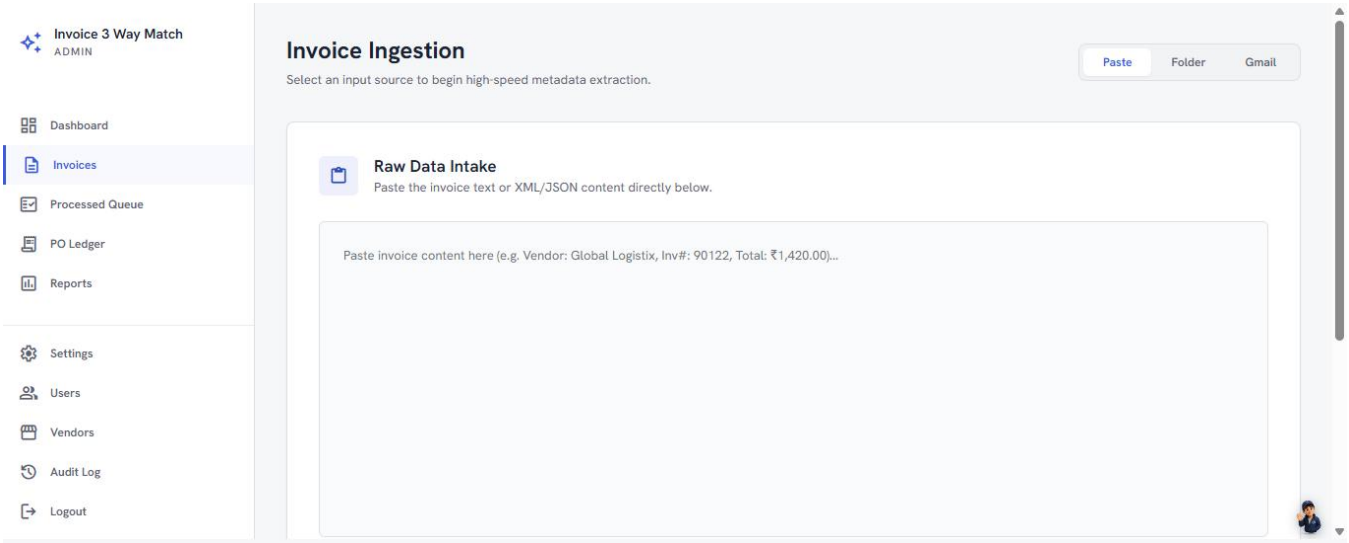
<- Back to Table of Contents

This is the day-to-day workflow: getting invoices into the system, reviewing what the AI extracted, and resolving anything that doesn't match cleanly. Admins have this exact same capability, plus the admin-only screens covered in the Admin Guide.

Getting an invoice in

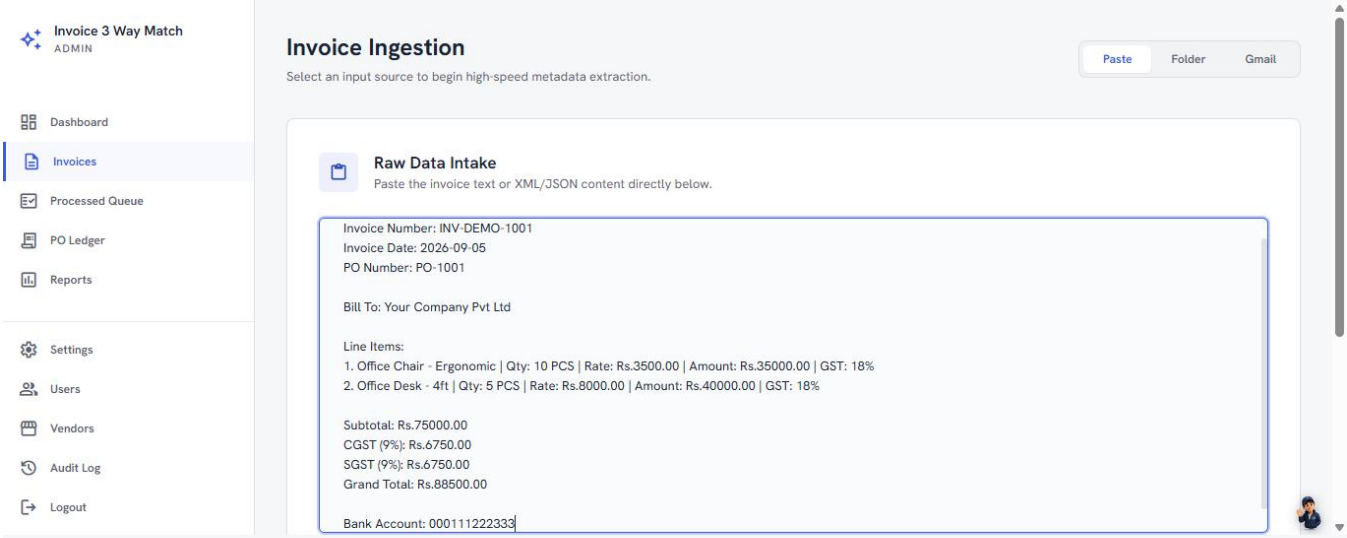
From **Invoices** in the sidebar, there are three ways in:

- **Paste** — paste the raw invoice text directly.
- **Folder** — upload a PDF or image file.
- **Gmail** — pull invoices in automatically from a connected mailbox (set up by your admin — see Settings Reference).



Raw Data Intake, empty

Paste or upload the invoice, then extract:



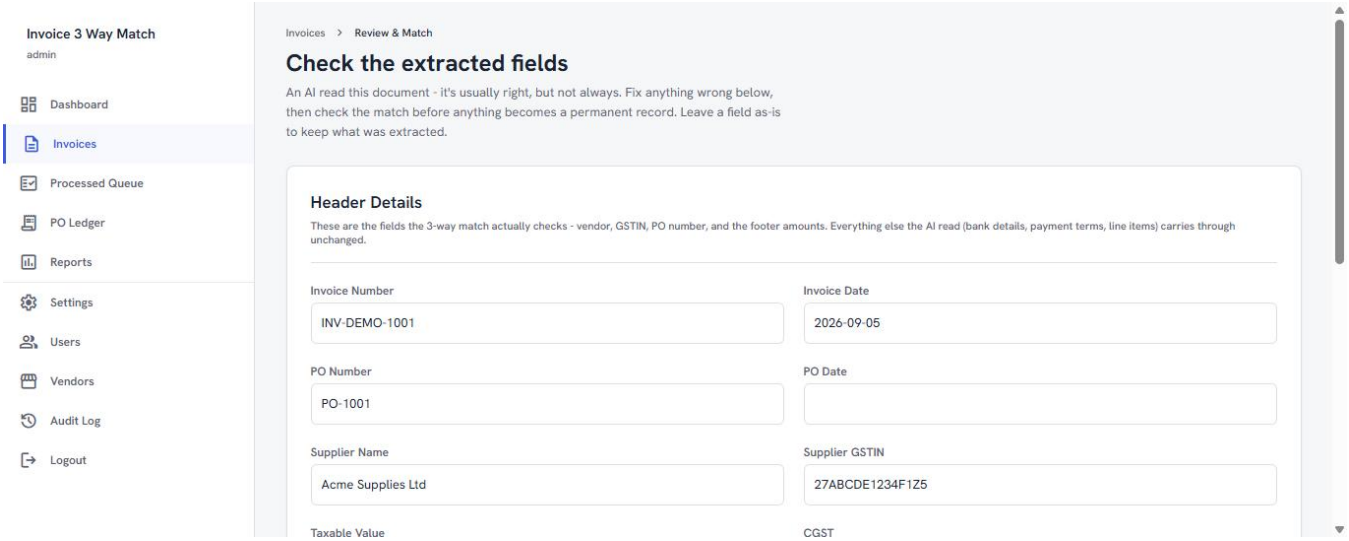
Raw Data Intake, filled in

Do: paste the actual invoice text/document, not a summary or your own description of it — the AI reads what's actually there.
Don't: worry about getting every field perfect before extracting — you'll get a chance to fix anything wrong on the very next screen.

Credit notes aren't accepted here. This app only does 3-way matching (PO vs. goods receipt vs. a payable invoice) — a credit note reduces an *existing* invoice's balance rather than creating a new payable, so it's a different workflow entirely and is rejected at extraction. A document clearly titled "Credit Note" is turned away outright; one framed as a regular invoice but showing a negative total is caught the same way. Apply credit notes against the original invoice wherever your payables ledger lives instead.

Reviewing what the AI read

Every extraction lands on the **Review & Match** screen before anything is saved. Nothing becomes a permanent record until you explicitly confirm it.

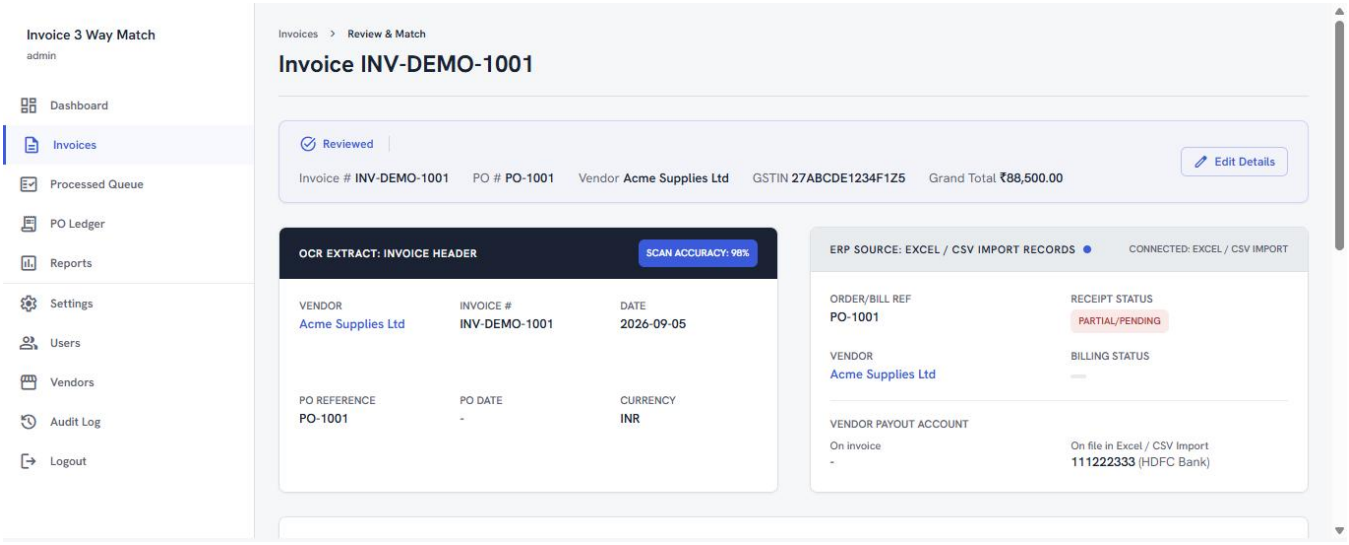


Review screen, extracted fields

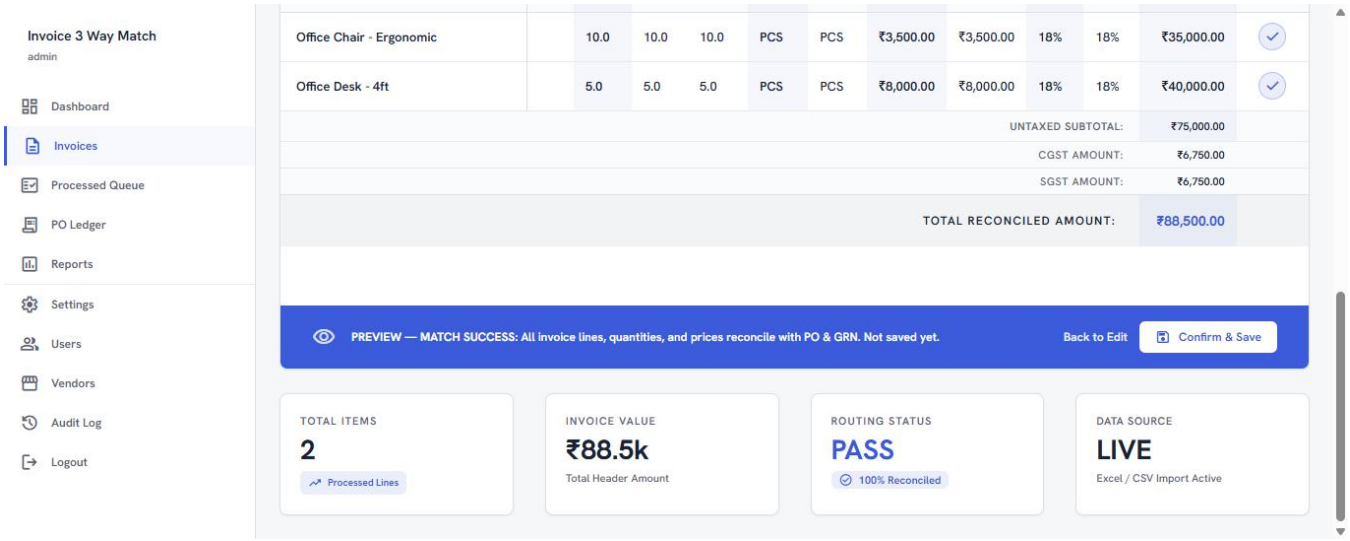
The fields shown here (Invoice Number, PO Number, Supplier Name/GSTIN, and the five footer amounts) are the ones the 3-way match actually checks — fix anything the AI got wrong. Line items are shown for reference only and aren't editable here; if a line item itself is wrong, discard the extraction and re-submit a clearer copy of the invoice instead.

> **Do:** actually read this screen, especially for a low-confidence extraction (blurry scan, unusual invoice layout) — the AI is usually right, but "usually" isn't "always".
> **Don't:** blindly click through to Check Match without glancing at the Supplier Name and PO Number — a wrong PO number here means matching against the wrong purchase order.

Click **Check Match** to see a live preview — nothing is saved yet:

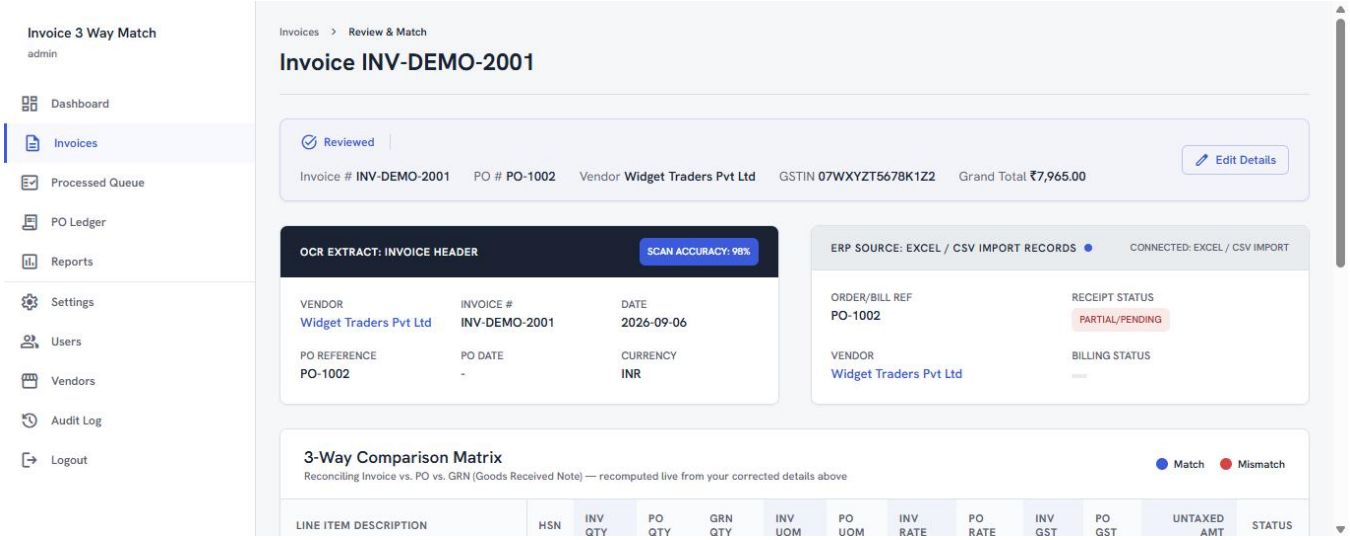


Match preview - a clean match

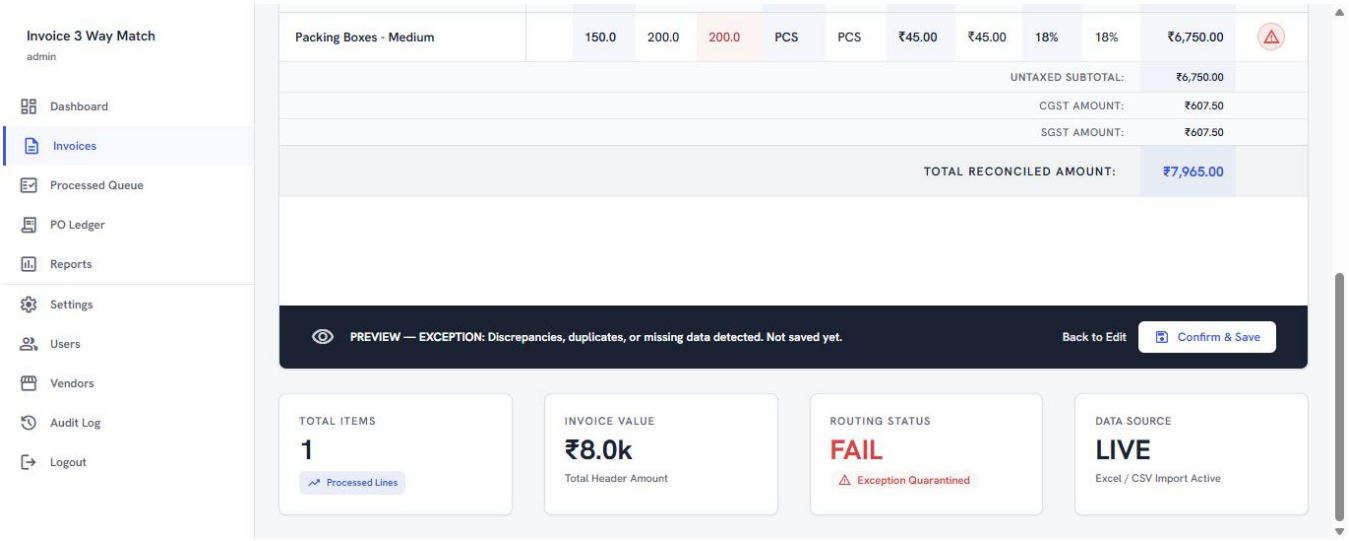


Match preview - reconciled totals

If everything lines up, you'll see **"MATCH SUCCESS"** and a **Confirm & Save** button. If it doesn't, you'll see **"EXCEPTION"** instead, with the specific mismatch highlighted:



Exception preview - quantity mismatch



Exception preview - routing status

In the example above, the invoice states 150 units but the purchase order shows 200 ordered and received — a genuine quantity discrepancy worth checking with the vendor before paying. You can still **Confirm & Save** an exception — it lands in the Processed Queue as an Exception for someone to resolve, rather than being blocked outright.

> **Do:** use **Back to Edit** if you spot a mistake in the header fields after checking the match — you can correct and re-check as many times as you need before saving. Only the *final* check before Confirm & Save is what gets logged.

The Review Queue (Gmail invoices needing a second look)

Gmail ingestion is hands-off by design — most invoices it scans go straight into the Processed Queue as Matched or as an Exception, without anyone clicking through the Review & Match screen. There is one exception to that, and it's deliberate: if a Gmail-ingested invoice trips one of the fraud checks below — a duplicate invoice number, same-PO re-billing, a vendor-identity or bank-account mismatch — it is **not** saved anywhere. It's held in the **Review Queue** instead:

Vendor / Invoice # / Amount	What the AI read off the invoice
Flagged As	Which fraud check fired
Received	When the scan picked it up

The sidebar shows a red badge with the number waiting. Click **Review** on a row and you land on the same **Review & Match** screen described above, with the same mandatory override-reason gate: you cannot save a flagged invoice without typing a reason, exactly as if you'd pasted it in by hand. **Discard** throws it away without saving anything.

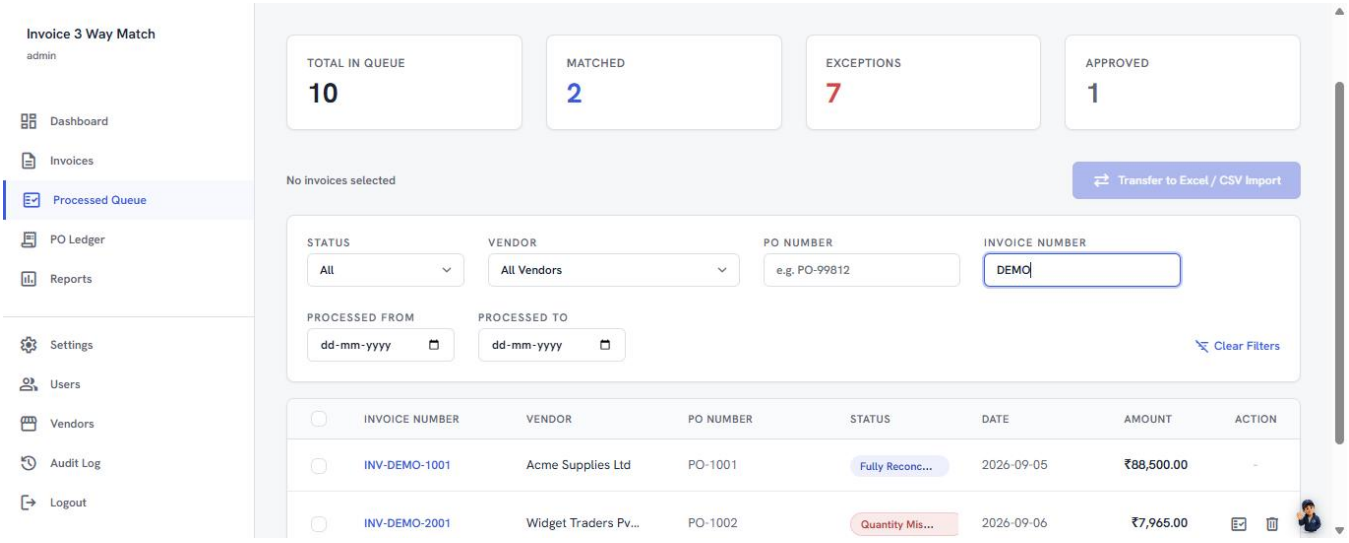
Nothing in this queue exists as a record yet — it isn't in the Processed Queue, it isn't in any report, and it hasn't been counted against its PO. Leaving a row here (closing the tab, navigating away mid-review) is safe: it stays put for you or anyone else to pick up again.

> **Do:** treat this queue as a real worklist, not a notification. An invoice sitting here is a bill nobody has accepted or rejected — the vendor is still waiting, and the duplicate question is still open.
> **Don't:** assume a quiet Review Queue means Gmail found nothing — ordinary mismatches (a quantity or price discrepancy, a PO that couldn't be found) still auto-commit to the Processed Queue as Exceptions and never appear here.

A small amber "No E-Invoice IRN" or "IRN Format Unusual" badge can appear next to the match result, independent of whether the invoice matched or became an exception. This only checks whether the invoice carries a properly-formatted e-invoice IRN (Invoice Reference Number) — it does **not** verify the invoice against the government e-invoice portal, and doesn't confirm an IRN hasn't been cancelled. A missing IRN does **not** by itself mean the vendor is non-compliant — only businesses above Rs. 5 crore turnover are required to e-invoice, and this app has no way to know a given vendor's turnover. Treat it as a prompt to verify with the vendor, never as a fraud finding — it never blocks Confirm & Save. The Duplicate & Fraud Risk Report (under Reports) rolls every flagged invoice up into one place, along with the tax amount involved.

The Processed Queue

Every invoice you've confirmed — Matched or Exception — lands here, along with everything Gmail ingestion committed on its own. This is the one worklist for everything already through extraction:



Processed Queue

Use the filters (Status, Vendor, PO Number, Invoice Number, date range, **E-Invoice Risk Only**) to narrow down a long list. Each row's action icons let you:

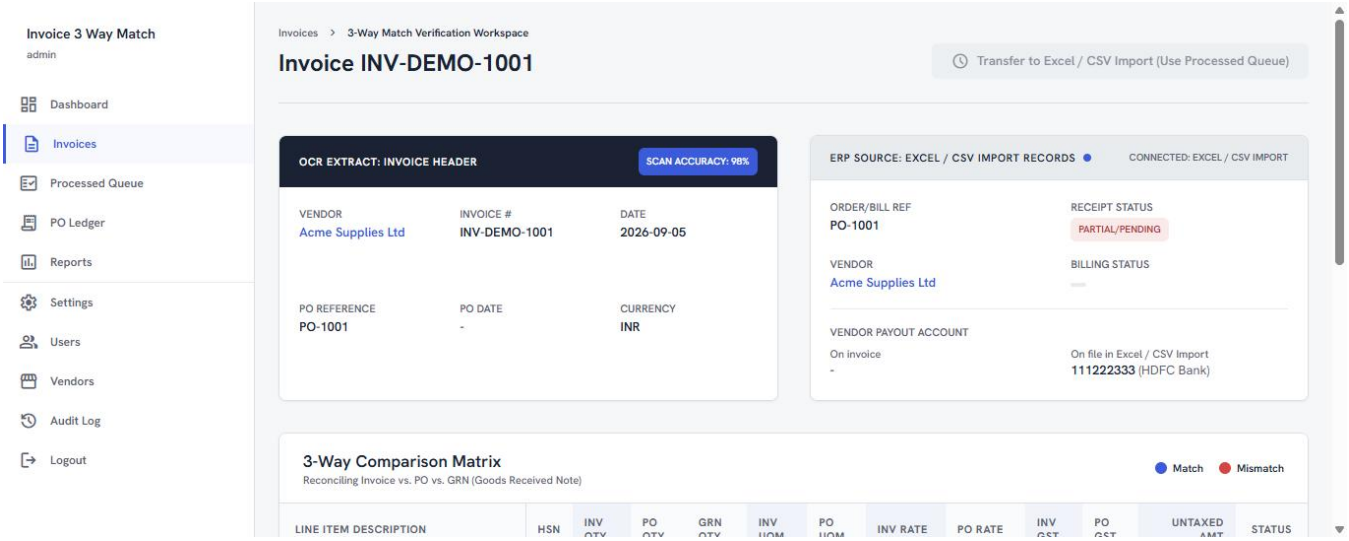
- **Approve with a note** (Exception rows only) — for a mismatch you've checked and decided

is genuinely fine (e.g. a vendor's since-corrected GST number). You're required to type a short reason, which is kept on the record and in the Audit Log permanently. This does **not** silently fix the underlying data — it's a documented, auditable sign-off that this specific exception doesn't need to block anything further.

- **Delete** (Exception rows only) — permanently removes an exception you've determined isn't a real invoice or was a genuine mistake. Matched invoices can never be deleted from here — they're kept as a permanent record.

> **Don't** approve-with-note as a way to make an exception disappear without actually checking it — the note is visible to anyone who looks at that invoice later, including in the Audit Log. A vague note like "ok" defeats the entire point of the control.

Once an invoice is saved:



A confirmed, matched invoice

Transferring to your backend

Select one or more **Matched** invoices in the Processed Queue and use **Transfer to [your backend]** to push them into your connected system (Odoo, Zoho, etc.) — the exact button label matches whichever backend your admin has configured (see Settings Reference). Not every backend supports this yet — some connectors are read-only for now, in which case the invoice stays recorded here as Matched, just not automatically pushed elsewhere.

> **Do:** resolve any Exception sharing the same PO number before transferring a Matched invoice against it — the system blocks this deliberately (a disabled checkbox, with the reason shown) to stop a duplicate or over-billed PO from getting paid while a real question about it is still open.

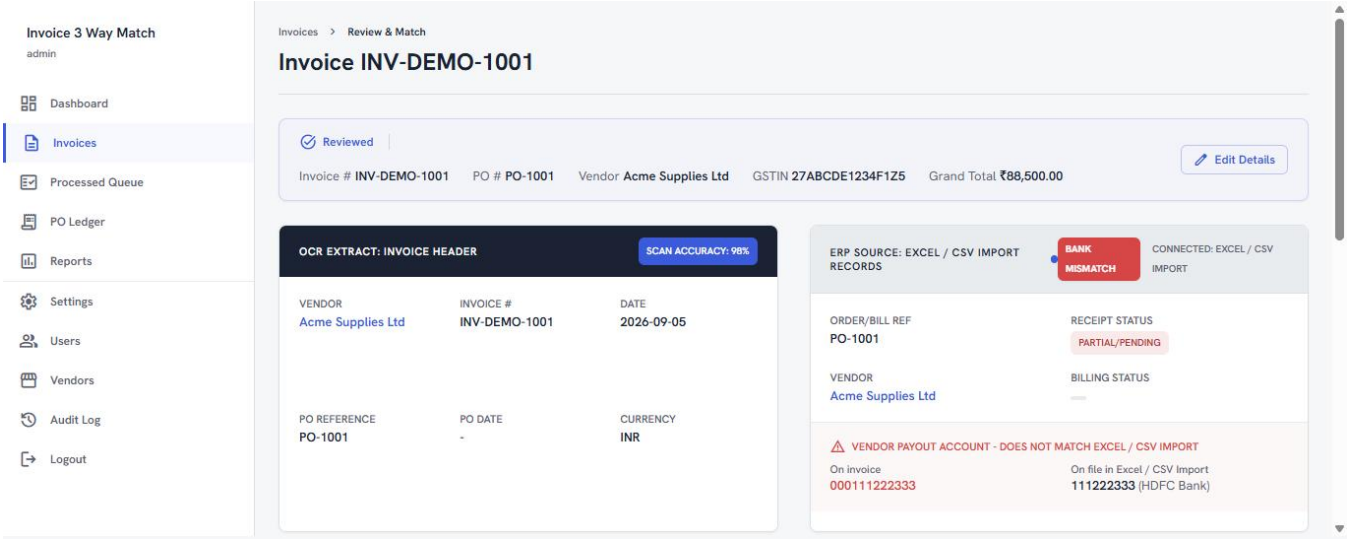
Fraud detection you can't turn off

A handful of checks run on every invoice regardless of your match rules/tolerance settings, because they're security controls, not data-quality preferences a company should be able to switch off. They also apply regardless of *how* the invoice arrived — an invoice that trips one of these can never be saved without a typed override reason, whether you pasted it in yourself or Gmail ingestion found it (in which case it waits in the Review Queue until someone does exactly that):

• **Duplicate invoice numbers** — the exact same invoice number seen before (Matched, Exception, or Approved) is flagged immediately.

• **Same-PO re-billing** — a suspiciously similar amount billed again against a PO already billed once, even under a different invoice number.

• **Vendor bank-account mismatch** — if the invoice states a payout account that doesn't match what's on file for that vendor, you'll see this:



Bank mismatch example

This is exactly the kind of thing a fraudster gets right on everything *except* the payout account — notice in the example above every line item and the footer total matched perfectly, and it was still correctly held as an Exception.

> **Don't** override a bank-mismatch exception without actually calling the vendor on a known, previously-used phone number to confirm the change — never a number or contact provided in the same suspicious invoice.

Where to go next

• Admin-only screens (Users, Vendors, Audit Log, License): Admin Guide

• Everything you can view but not change: Viewer Guide

Viewer Guide

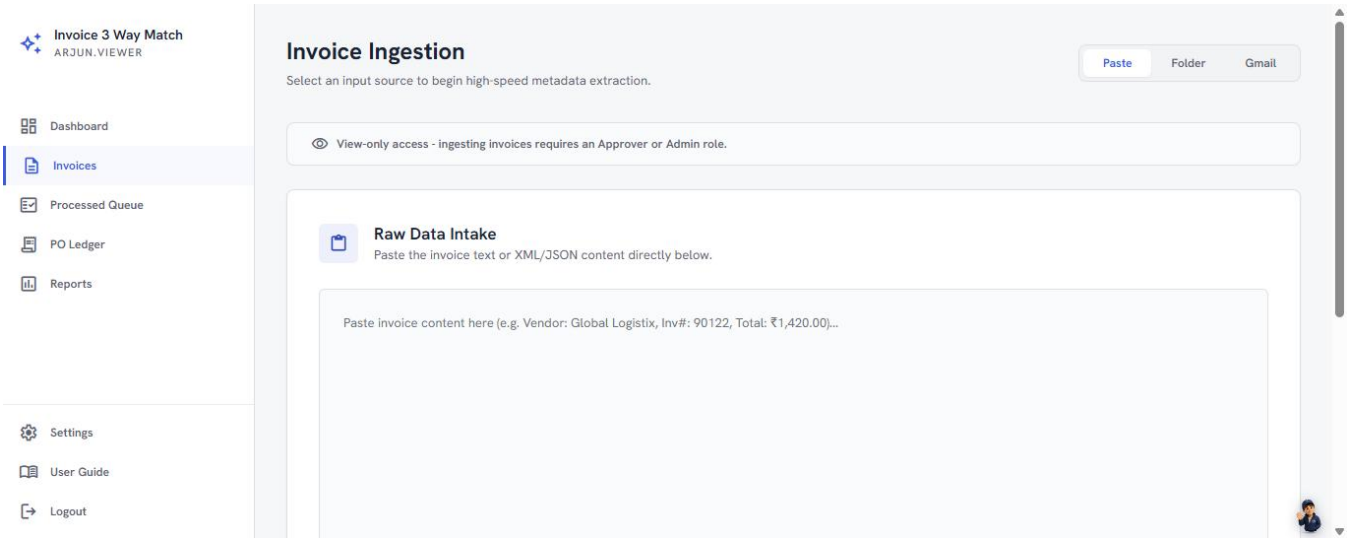
<- Back to Table of Contents

Viewers can see almost everything Approvers and Admins can, but can't change any of it. This is the right role for someone who needs to monitor AP activity — finance leadership, an auditor, someone covering for an Approver on holiday — without being able to touch the data.

What's different about your sidebar

Your sidebar is shorter than an Approver's or Admin's: no Users, Vendors, or Audit Log links, because those screens don't exist for you at all (not just greyed out — the routes themselves refuse a Viewer).

If you open **Invoices** anyway (e.g. from a bookmark), you'll see it, but it's inert:



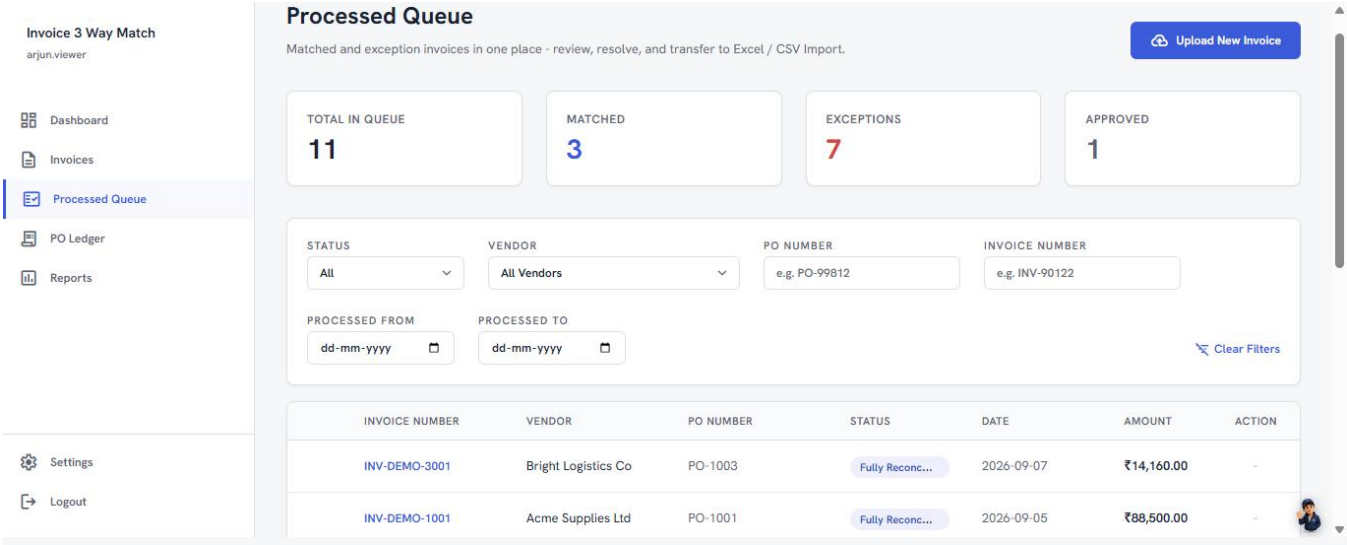
Invoice ingestion, view-only

A banner tells you plainly why: *"View-only access - ingesting invoices requires an Approver or Admin role."* Nothing on this screen will save.

> **Do:** ask an Approver or Admin to ingest an invoice for you if one needs to go in — that's not a Viewer capability, by design.
> **Don't:** waste time pasting an invoice here expecting it to process — it won't.

The Processed Queue — read, not act

You can open the Processed Queue and use every filter (Status, Vendor, PO Number, Invoice Number, date range) exactly like an Approver does. The one difference is the **Action** column:



Processed Queue, no action icons

Where an Approver sees approve/delete icons on Exception rows, you see a dash (**–**) — the icons simply aren't rendered for your role. The row data itself (status, amounts, mismatch reasons) is fully visible.

> **Do:** use this queue to monitor how many exceptions are piling up, or to check on a specific vendor/PO — that's exactly what this role is for.
> **Don't:** ask someone to "just quickly action this from your screen" as a workaround — if you need approval authority regularly, ask your admin for an Approver account instead (see Admin Guide -> Managing users).

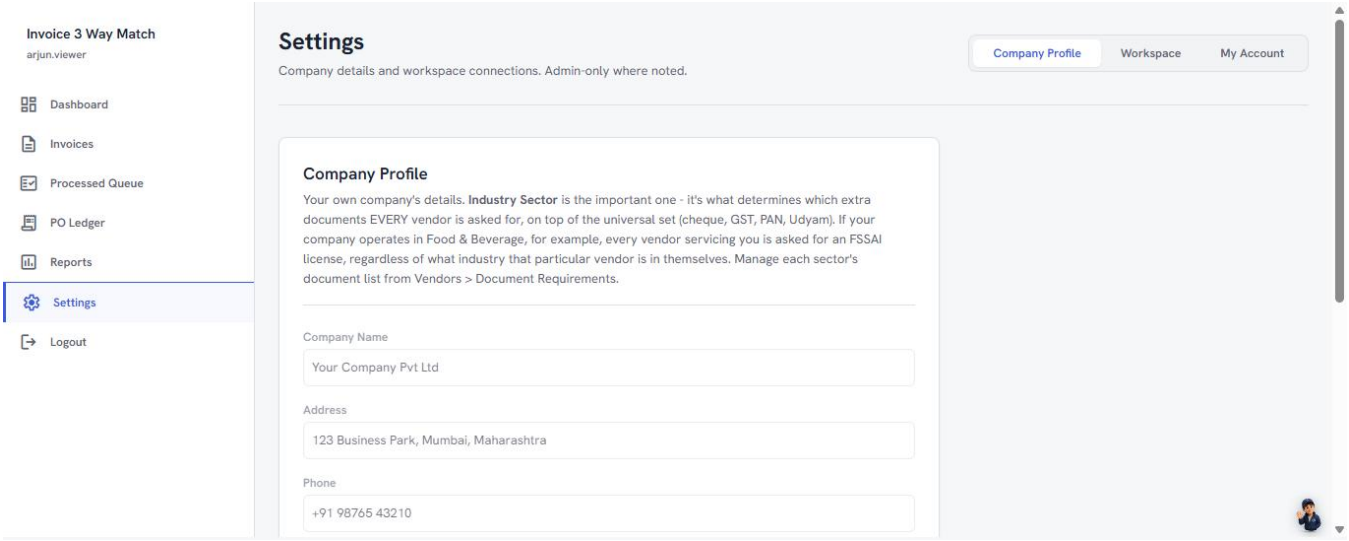
Dashboard and PO Ledger

Both work identically to what's described in Getting Started — the KPI tiles, status-mix chart, top vendors, and the PO Ledger table are all fully visible to you. You just won't see an upload control on the PO Ledger page; uploading a new ledger file requires Approver or Admin.

If anything has tripped a duplicate, re-billing, or vendor-identity/bank fraud check (see Approver Guide -> Fraud detection you can't turn off) and is still unresolved — including a Gmail-ingested invoice an Approver hasn't reviewed yet — you'll see a red **Fraud Risk Alert** banner at the very top of the Dashboard, above everything else. You can see exactly what was flagged and why, with a link straight to the full Duplicate & Fraud Risk Report. You won't see a **Review/View** action link next to each item — that's an Approver/Admin action — but nothing about a flagged invoice is hidden from you.

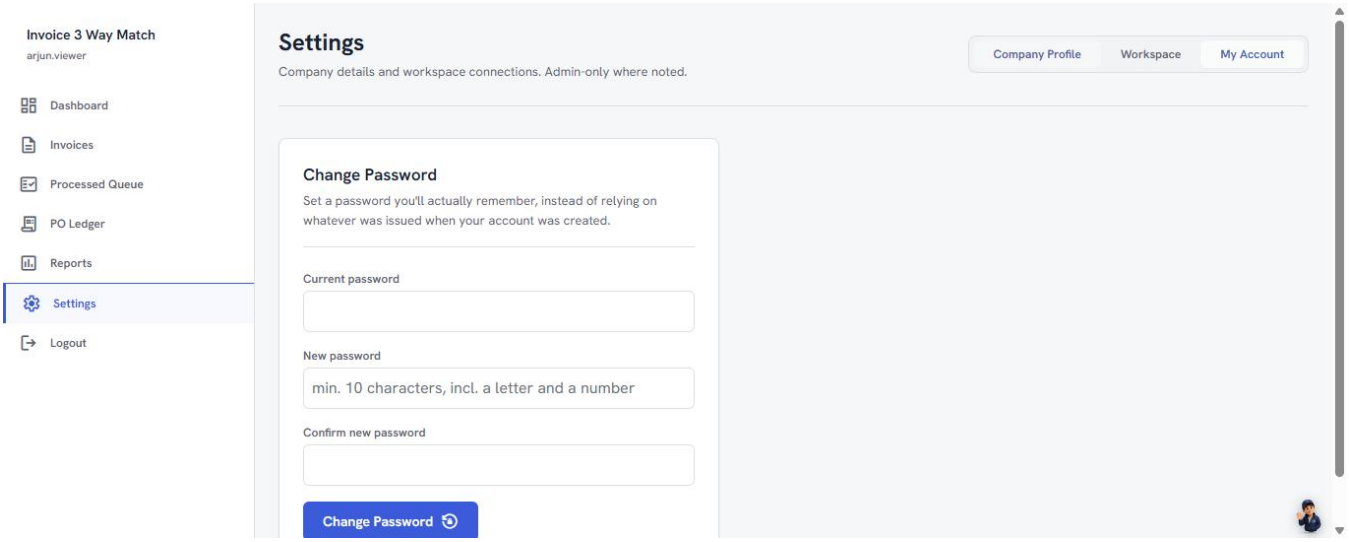
Settings — visible, but nothing saves

Every tab (Company Profile, Workspace, My Account) opens for you, so you can see current configuration for reference:



Settings, Company Profile as a Viewer

Almost everything on it is greyed out and can't be clicked into or typed into at all — this isn't just a warning shown after the fact, the fields themselves are switched off for your role. The one exception is your own password, which every role can change for themselves:



Change Password, available to every role

Do: treat Settings as a reference screen — useful for checking "which AI provider is configured?" or "what's our seat count?" without needing to ask an Admin.
Don't: try to work around the greyed-out fields — Company Profile, connector credentials, and everything else here are locked for a reason. Ask your Admin to make the change instead (see Admin Guide and Settings Reference).

Where to go next

- Full day-to-day workflow (what an Approver can additionally do): Approver Guide
- Every admin-only screen: Admin Guide
- Every Settings field explained in full: Settings Reference

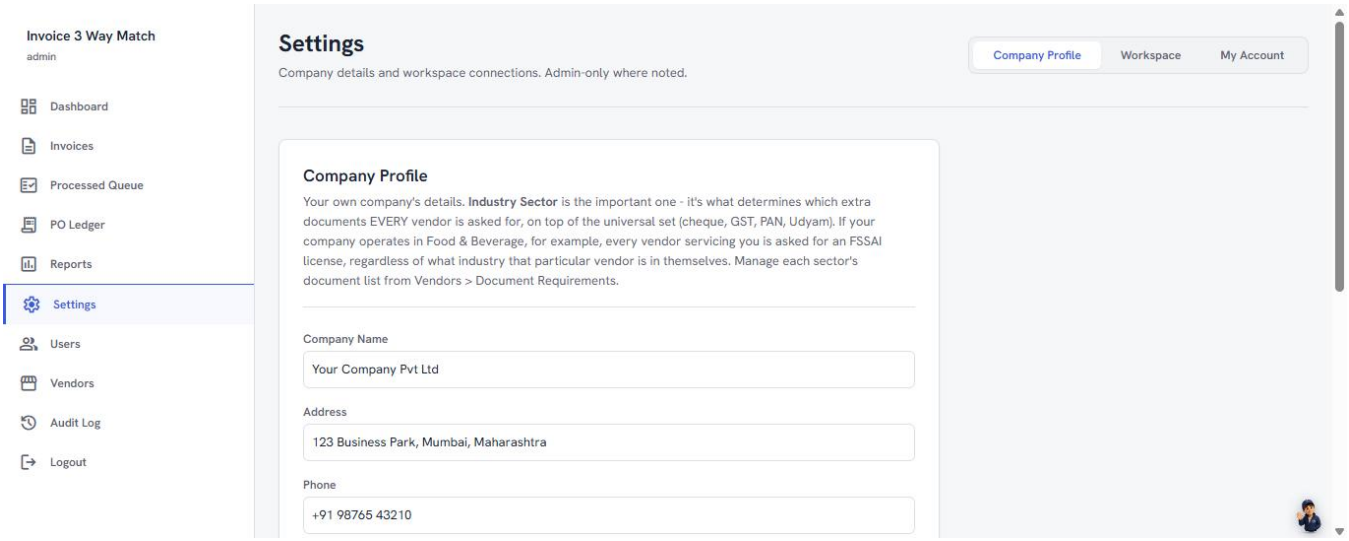
Settings Reference

<- Back to Table of Contents

Every field on every Settings screen, explained. This chapter is for Admins — Approvers and Viewers can open these screens too (see the Viewer Guide for what that looks like), but only Admins can actually save most of what's here. Two topics get their own dedicated chapter because there's enough to say: AI Provider & Local Model Setup and Single Sign-On Setup.

Settings has three tabs: **Company Profile**, **Workspace**, and **My Account**.

Company Profile

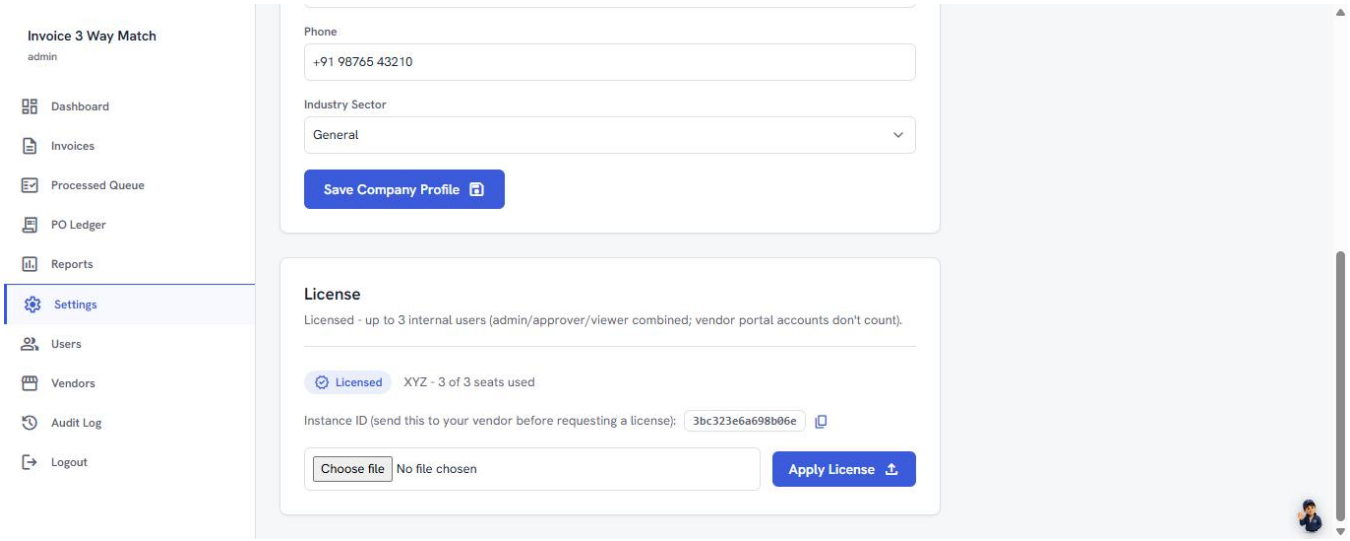


Company Profile tab

- **Company Name / Address / Phone** — cosmetic, shown on your own side only; not sent anywhere or used in matching logic.
- **Industry Sector** — the one field here that actually changes behavior. It determines which *extra* documents every vendor of yours is asked for, on top of the universal set (cancelled cheque, GST Certificate, PAN Card, Udyam). Manage each sector's extra list from **Vendors -> Document Requirements** (admin-only — see Admin Guide).

Scrolling down on this same tab also shows the license status:

License



License section

• The badge (**Licensed** / trial / expired) and seat usage (`X of Y seats used`) reflect your current install.

• **On a trial**, the card also shows how much evaluation you have left. There are two limits and whichever runs out first ends the trial: **30 days**, or **100 invoices** actually saved to the Processed Queue. Looking at a match without confirming it doesn't count toward the invoice figure. Every feature is unlocked during the trial, with no limit on how many users you create.

• **Instance ID** is unique to this installation — send it to your vendor when requesting a license; a license file generated for a different Instance ID is rejected outright with an error naming your correct one. It **changes if you rebuild or move the server**, so you'll need a replacement license file when that happens — your vendor can look up what you previously bought and reissue it.

• If you have **more active users than your license covers**, a warning appears here and on the Users page, counting down **10 days**. This normally only happens right after a trial ends, because the trial has no limit on how many users you create — so if you made 10 accounts while evaluating and then bought 5 seats, you'll see it straight away.

During those 10 days nothing changes: everyone keeps working and nothing is switched off. To resolve it, either deactivate enough accounts on the Users page, or ask your vendor for more seats. After 10 days, **making changes is paused** until you do one of those — you can still view everything, nobody is deactivated for you, and nobody is signed out. Deactivating a user and applying a new license both keep working while changes are paused, so you're never stuck.

• **Apply License** installs a `.lic` file your vendor issued you. Applying one always works even if a previous trial or license has already expired — you're never locked out of the one action that would unlock you. Uploading the same file twice is harmless; the app simply tells you nothing changed.

• If you ever see **Needs attention** here instead of a trial or licensed badge, the app has found that its own licensing records don't add up — usually because something edited the database directly. Changes are paused (viewing still works). Send your vendor the Instance ID and they can sort it out.

> **Do:** copy the exact Instance ID shown here when asking for a license — a mistyped character means the file you get back won't validate.
> **Don't:** expect License section changes to need a Save button — applying a file *is* the save.

Workspace tab

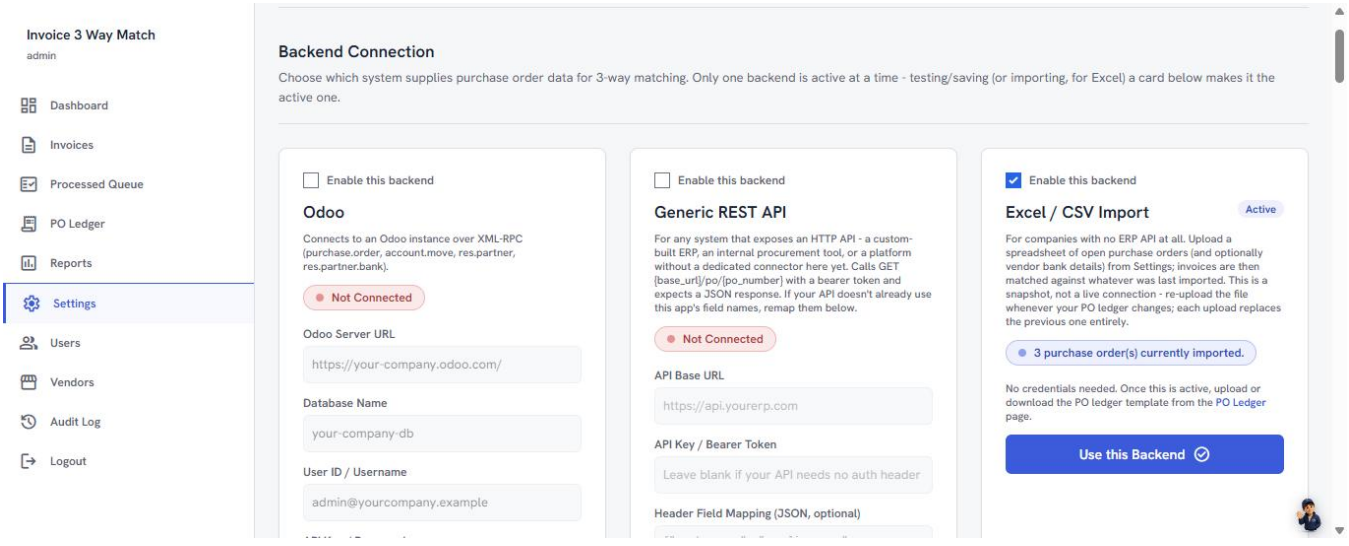
Backend Connection

This is where you tell the app **where your Purchase Orders and Goods-Received records come from**, so it has something to check each invoice against. You have four choices, shown as cards. **Only one can be switched on at a time** — turning one on switches the previous one off.

If you're not sure which one applies to you, or you don't use any of the named systems below (Odoo, Zoho Books, Tally): use **Excel/CSV Import**. It needs no setup, no technical knowledge, and no help from anyone else — see below.

> **Do:** whichever card you choose, click **Test & Save** (or **Use this Backend** for Excel/CSV Import) — nothing is saved until the test actually passes.
> **Don't:** switch between these casually once you're live — your PO Ledger and matching results follow whichever one is currently switched on; switching away and back doesn't restore anything, it just starts reading from whatever's active now.

Excel/CSV Import — the option for most people, no setup needed



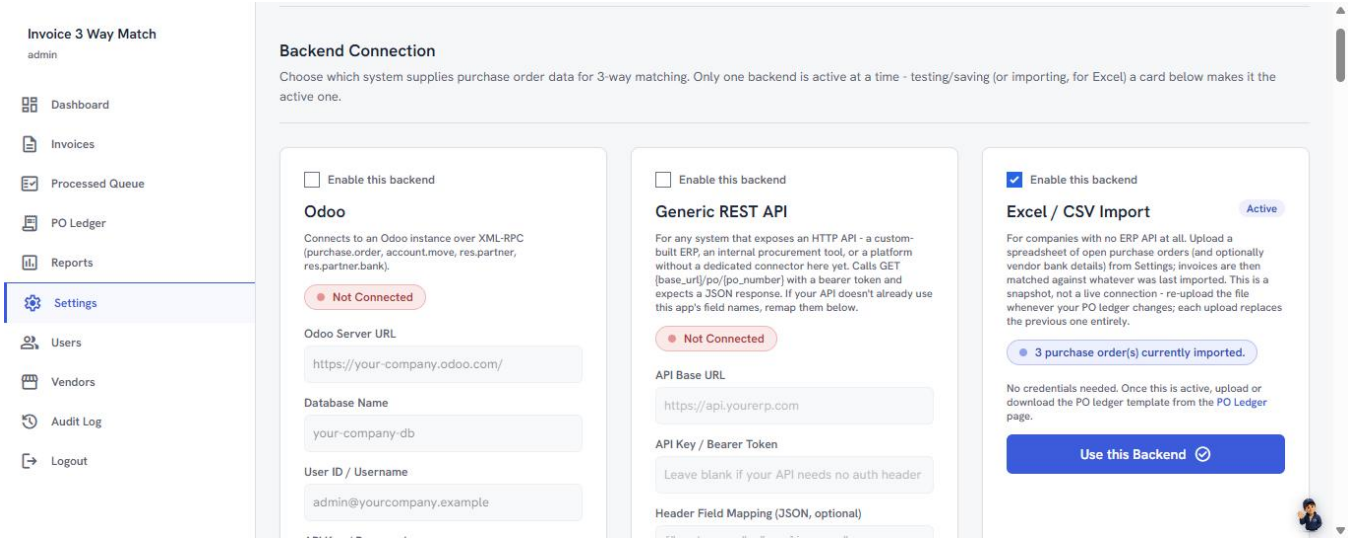
Excel/CSV Import card

If your company doesn't use one particular ordering system that this app can plug into directly, this is your option. You download a spreadsheet template, fill in your currently open purchase orders, and upload it here — no password, no technical account of any kind. Every invoice is then checked against whatever spreadsheet

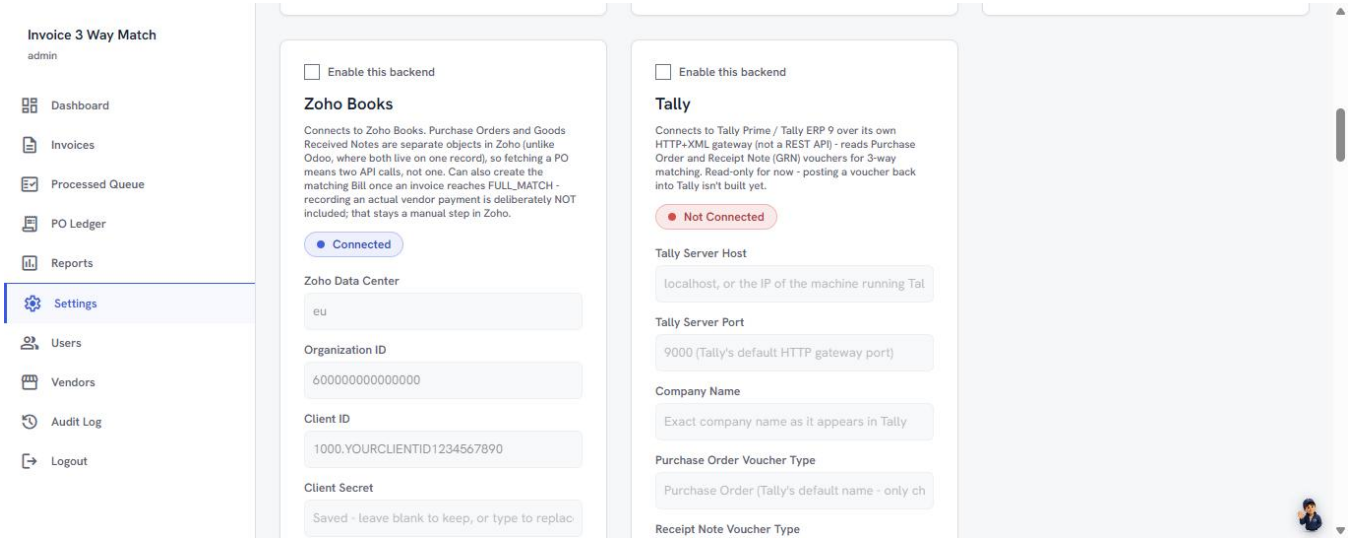
you last uploaded.

Keep in mind: **each upload completely replaces the previous one** — it doesn't add to it. Re-upload the whole file, with everything still open, every time your purchase orders change. See Getting Started for the upload walkthrough.

Odoo, Generic REST API, Zoho Books, Tally — if your company already uses one of these



Odoo and Generic REST API cards



Zoho Books and Tally cards

These four cards connect this app directly to a system your company may already use to manage purchase orders. Setting one of these up needs technical details (server addresses, account IDs, security keys) that only the person or company who manages that system will have — **this is not something you're expected to figure out yourself.**

> **Share this box with whoever manages that system for your company** — your own IT person, or that system's own support team/vendor if you don't have in-house IT. They'll know what each of these fields means and where to find the right values.
> - **Odoo**: needs the Odoo server's web address, the database name, a username, and an API key or password for that account. Ask your Odoo administrator for these.
> - **Generic REST API**: for any custom or in-house system with its own way of sharing data over the internet, not one of the named systems above. Needs a web address and a security key ("bearer token") from whoever built or manages that system. If that system doesn't already use this app's exact field names, the optional "Field Mapping" boxes let a technical person tell this app which of their fields match which of this app's fields — skip these if the connection works without them.
> - **Zoho Books**: needs a Data Center region, an Organization ID, and a Client ID/Client Secret/Refresh Token — three separate security keys generated from Zoho's own developer settings. Ask whoever manages your company's Zoho Books account, or Zoho's own support, to generate these for you.
> - **Tally**: needs the address and port number of the computer running Tally on your network, your company name exactly as Tally has it, and the names Tally uses for your Purchase Order and Receipt Note voucher types. Ask whoever manages Tally on your network. Tally is **read-only** here — this app can read your Tally data to check invoices against, but doesn't write anything back into Tally.

Once whoever manages the relevant system has these details, come back to this page, fill them into the matching card, and click **Test & Save**.

AI Provider

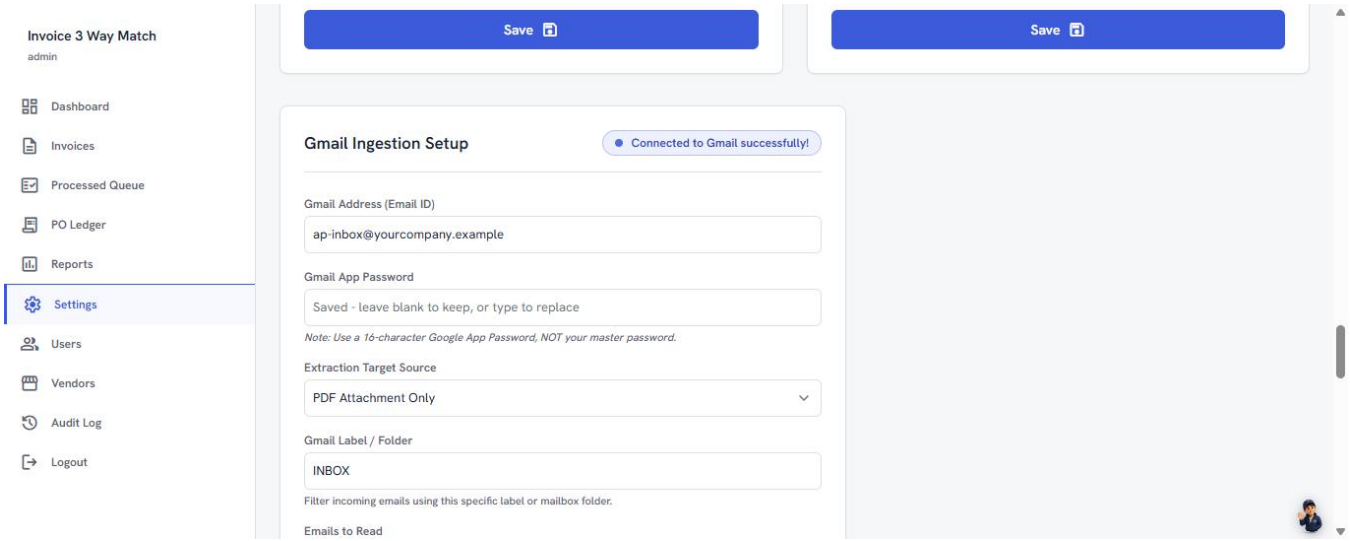
Covered in full in its own chapter: AI Provider & Local Model Setup.

Single Sign-On

Covered in full in its own chapter: Single Sign-On Setup.

Gmail Ingestion Setup

Lets Approvers and Admins pull invoices straight from a mailbox instead of pasting/uploading them one at a time (see Approver Guide):



Gmail Ingestion Setup

• **Gmail Address** — the mailbox to read invoices from. This does **not** have to be any individual person's own inbox — a dedicated shared mailbox (e.g. an `ap-invoices@` address) is the better choice, since this same mailbox is also where any **vendor invite drafts** get created (see Admin Guide -> Managing vendors) — whoever's inbox this is becomes the "from" identity for everything this app sends through Gmail.

• **Gmail App Password** — see **Getting a Gmail App Password** below. This is **not** your normal Gmail password — your regular password will not work here.

• **Extraction Target Source** — whether to read the email's own text, a PDF attached to it, or both.

• **Gmail Label/Folder** — only scan a specific folder/label instead of the whole inbox (leave blank to scan the main inbox).

• **Emails to Read** — every unread email, or only ones matching the label above.

• **Load Demo Gmail** — fills in a working demo mailbox so you can see the whole feature working before connecting your own — a good way to try this out risk-free first.

Once an email has been read, this app automatically labels it "Processed" in that mailbox, so the same email is never read twice.

Getting a Gmail App Password

A Gmail App Password is a special 16-character code that lets this app read a specific mailbox, without ever knowing that account's real password. Google requires this for any outside application connecting to Gmail this way — it cannot be skipped.

If you don't manage this Google account yourself, share this box with whoever does (your IT person, or whoever owns the mailbox you're connecting) — they'll need to be signed into that Google account to do this.

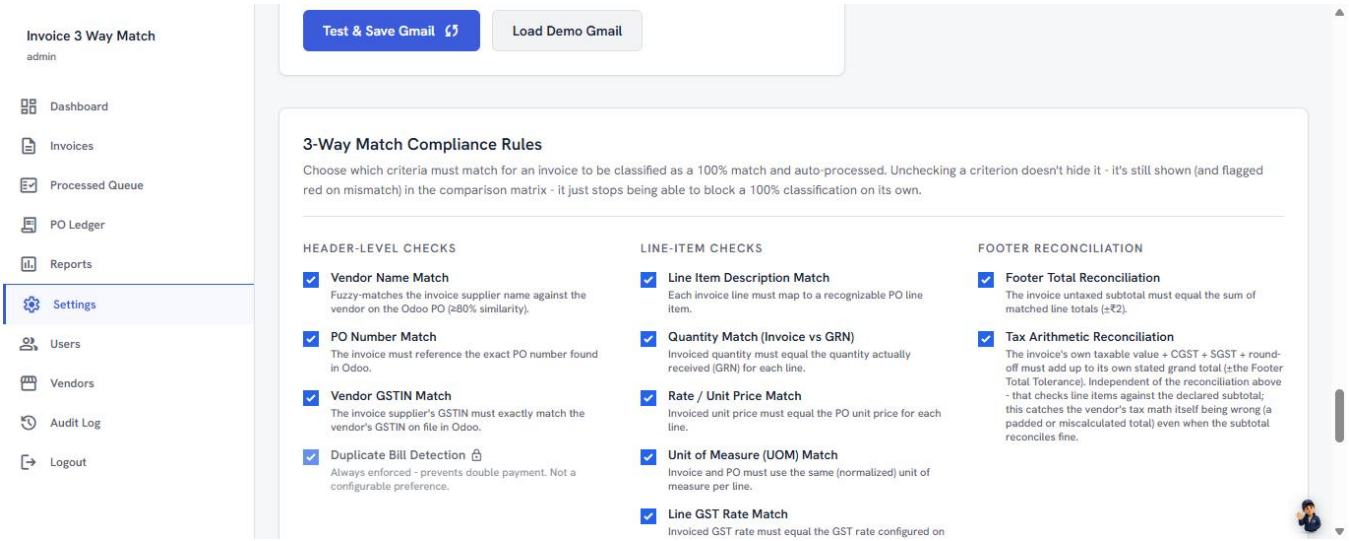
1. **Turn on 2-Step Verification first, if it isn't already on** — an App Password can't be created without it. Go to myaccount.google.com/security and turn on **2-Step Verification** if you see it's off.
2. Go directly to myaccount.google.com/apppasswords and sign in again if asked.
3. Type a name for it — anything that reminds you what it's for, e.g. "3 Way Match" — and click **Create**.
4. Google shows a **16-character password** in a yellow box, e.g. `abcd efgh ijkl mnop`. Copy it exactly (the spaces don't matter either way).
5. Paste it into the **Gmail App Password** field in this app's Settings and click **Test & Save Gmail**.

This code is shown by Google only once — if you lose it, you can't retrieve it again, only create a new one the same way.

Do: use a dedicated mailbox rather than a real person's inbox for this — see the note above about vendor invites.
Don't: paste your normal Google account password into the **Gmail App Password** field — it will not work, and typing your real password into any third-party app's password field is exactly the kind of thing to avoid as a habit.

3-Way Match Compliance Rules

Choose **which** criteria must match for an invoice to be classified as a 100% match and auto-processed. Unchecking a criterion doesn't hide it — it's still shown (and still flagged red on a mismatch) in the comparison matrix on the Review screen; unchecking it only stops that one criterion from being able to block a 100% classification by itself.



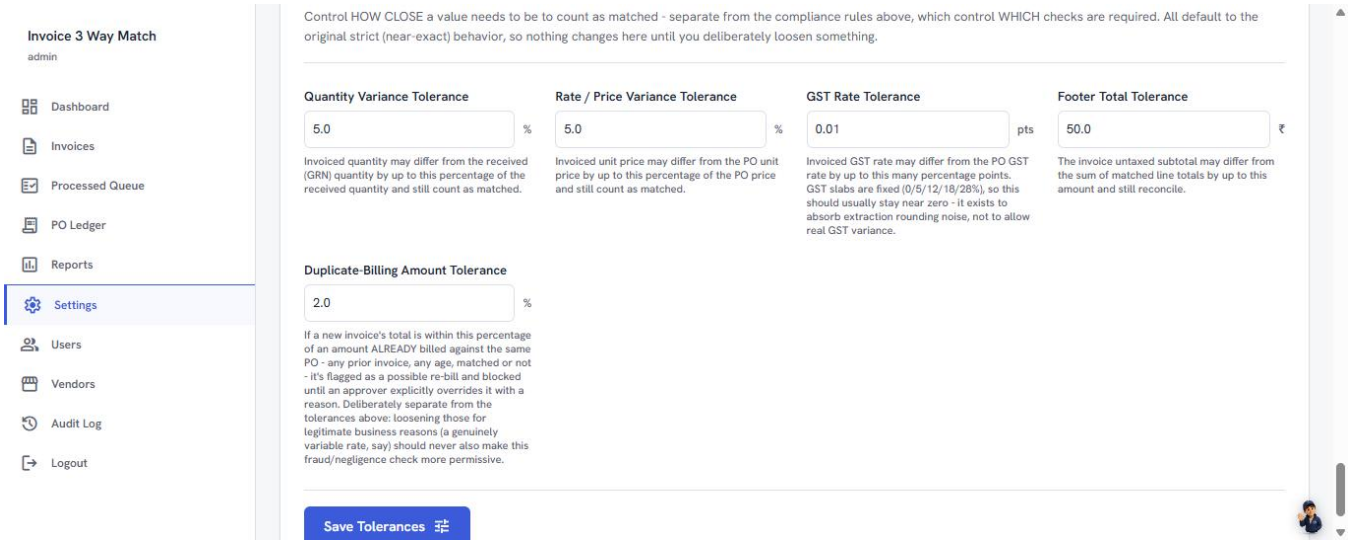
3-Way Match Compliance Rules

Check	What it verifies
Vendor Name Match	Fuzzy-matches the invoice supplier name against the vendor on the PO (>=80% similarity).
PO Number Match	The invoice must reference the exact PO number found in your backend.
Vendor GSTIN Match	The invoice supplier's GSTIN must exactly match the vendor's GSTIN on file.
Duplicate Bill Detection	Always enforced — not a configurable preference. Prevents double payment.
Line Item Description Match	Each invoice line must map to a recognizable PO line item.
Quantity Match (Invoice vs GRN)	Invoiced quantity must equal the quantity actually received.
Rate / Unit Price Match	Invoiced unit price must equal the PO unit price for each line.
Unit of Measure (UOM) Match	Invoice and PO must use the same (normalized) unit of measure per line.
Line GST Rate Match	Invoiced GST rate must equal the GST rate configured on the PO line.
Footer Total Reconciliation	The invoice's untaxed subtotal must equal the sum of matched line totals.
Tax Arithmetic Reconciliation	The invoice's own taxable value + CGST + SGST + round-off must add up to its own stated grand total — catches the vendor's own tax math being wrong even when the subtotal reconciles fine.

Do: leave every check enabled unless you have a specific, understood reason to loosen one — each exists to catch a real class of billing error.
Don't: confuse unchecking a rule here with raising its *tolerance* — that's the separate section below. Unchecking says "don't require this"; a tolerance says "allow this much difference and still count it as matching."

Match Tolerances

Controls **how close** a value needs to be to count as matched — separate from the compliance rules above, which control *which* checks are required. Everything here defaults to strict, near-exact behavior; nothing changes until you deliberately loosen it.



Match Tolerances

• **Quantity Variance Tolerance** — invoiced quantity may differ from the received (GRN) quantity by up to this percentage and still count as matched.

• **Rate/Price Variance Tolerance** — invoiced unit price may differ from the PO unit price by up to this percentage and still count as matched.

• **GST Rate Tolerance** — invoiced GST rate may differ from the PO GST rate by up to this many *percentage points*. Since GST slabs are fixed (0/5/12/18/28%), this should normally stay near zero — it exists to absorb extraction rounding noise, not to allow genuine GST variance.

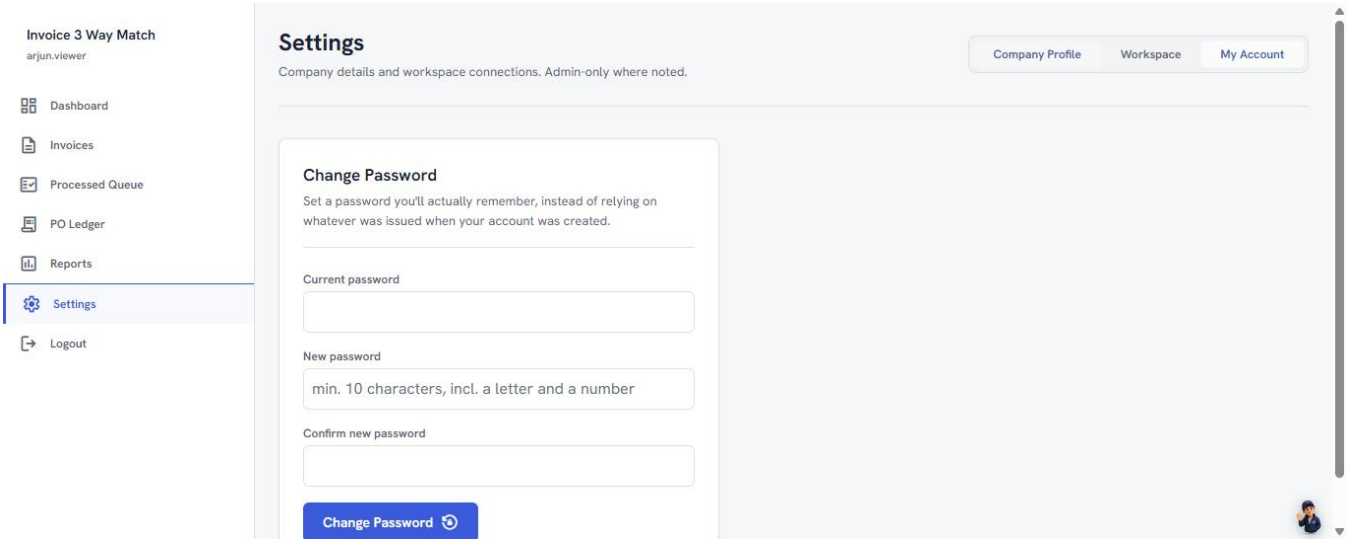
• **Footer Total Tolerance** — the invoice's untaxed subtotal may differ from the sum of matched line totals by up to this amount (Rs.) and still reconcile.

• **Duplicate-Billing Amount Tolerance** — if a new invoice's total is within this percentage of an amount *already* billed against the same PO (any prior invoice, any age, matched or not), it's flagged as a possible re-bill and blocked until an approver explicitly overrides it with a reason. Deliberately kept separate from the tolerances above: loosening those for legitimate business reasons (a genuinely variable market rate, say) should never also make this fraud/negligence check more permissive.

> **Don't** loosen the Duplicate-Billing tolerance to make a false-positive go away without checking why it fired first — see [Fraud detection you can't turn off](02-approver-guide.md#fraud-detection-you-cant-turn-off) for what this is actually guarding against.

My Account tab

Every role sees this tab, and it's the one Settings action available regardless of role:



Change Password

See Viewer Guide -> Settings for why this one action works for every role when nothing else on this page does.

Where to go next

• Choosing and configuring what actually reads your invoices: [AI Provider & Local Model Setup](06-ai-provider-setup.md)

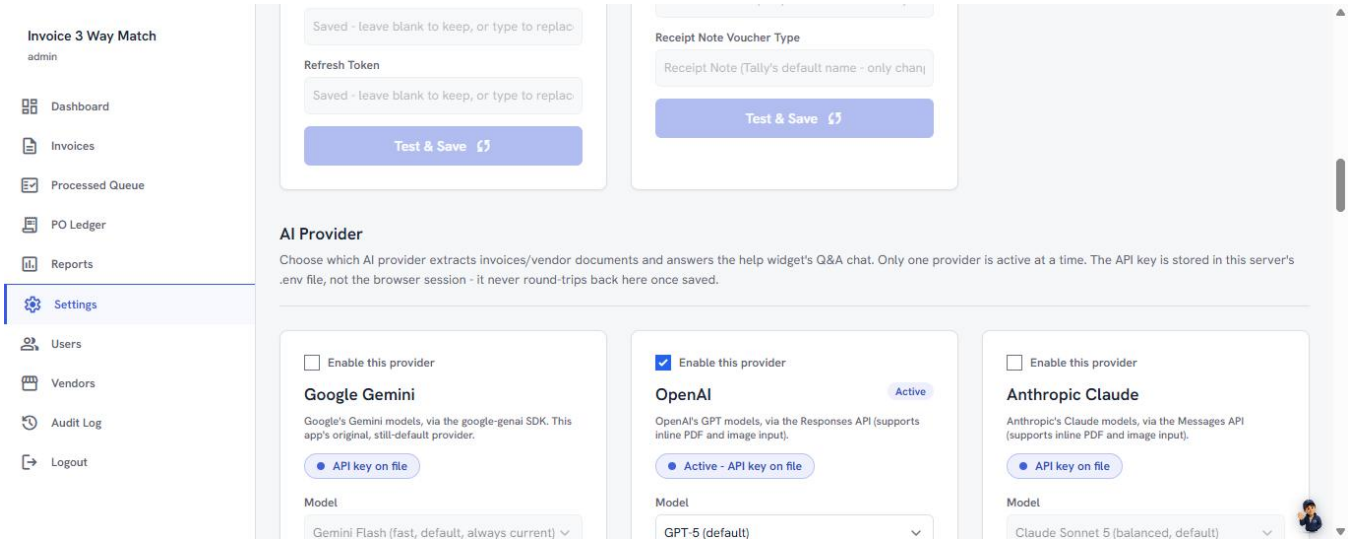
• Optional company login via Google/Microsoft: Single Sign-On Setup

• Everything admin-only outside of Settings (Users, Vendors, Audit Log): [Admin Guide](01-admin-guide.md)

AI Provider & Local Model Setup

<- Back to Table of Contents

This is Admin-only, and nothing can be extracted from an invoice until it's done at least once (step 4 of the first-time setup checklist). From **Settings -> Workspace -> AI Provider**:



AI Provider cards — Gemini, OpenAI, Anthropic Claude

Only one provider is active at a time. Whichever card you last successfully save becomes the one used for every invoice extraction and the in-app Help assistant's chat, everywhere in the app — there's no per-invoice or per-user choice.

The three hosted providers

Provider	Default model	Notes
Google Gemini	Gemini Flash	This app's original, still-default provider.
OpenAI	GPT-5	
Anthropic Claude	Claude Sonnet 5 (balanced)	

Each card's **Model** dropdown offers a small curated list (a fast/cheap option, a highest-quality option, and the default) plus **Custom model ID...**, which reveals a text field for typing any model name the provider supports that isn't in the curated list yet — useful the day a provider ships a newer model before this app's dropdown is updated to match.

Getting your first API key

If you've never done this before, **Google Gemini has the simplest, genuinely free starting point** of the three — no credit card required to get a working key. This is why it's this app's own default.

1. Go to aistudio.google.com and sign in with any Google

account (a personal Gmail account works fine — it doesn't need to be a company account).

2. Click **Get API key** (usually in the left-hand menu or top-right of the page).
3. Click **Create API key**, choosing "Create API key in new project" if asked.
4. Copy the key it shows you — a long string starting with `AIza...`. You won't need to come

back to this page again unless you lose it or want a new one.

Paste that value into the **Google Gemini** card's **API Key** field in this app's Settings, described below.

> **Do:** treat this key like a password — anyone who has it can use your Google account's quota. Only paste it into this app's own Settings screen.
> **Don't** expect Gemini's free tier to have no limits — it's rate-limited (a certain number of requests per minute/day), generous enough for a small team's normal invoice volume, but worth knowing about if extraction suddenly starts failing during a very high-volume day. If that happens, either wait for the limit to reset or switch to a paid tier from the same Google AI Studio page.

OpenAI and **Anthropic Claude** work the same way in spirit, but both require adding a payment method before they'll issue a working key (neither has a no-card free tier at the time of writing) — get a key from platform.openai.com/api-keys or console.anthropic.com respectively if you'd rather use one of those from the start.

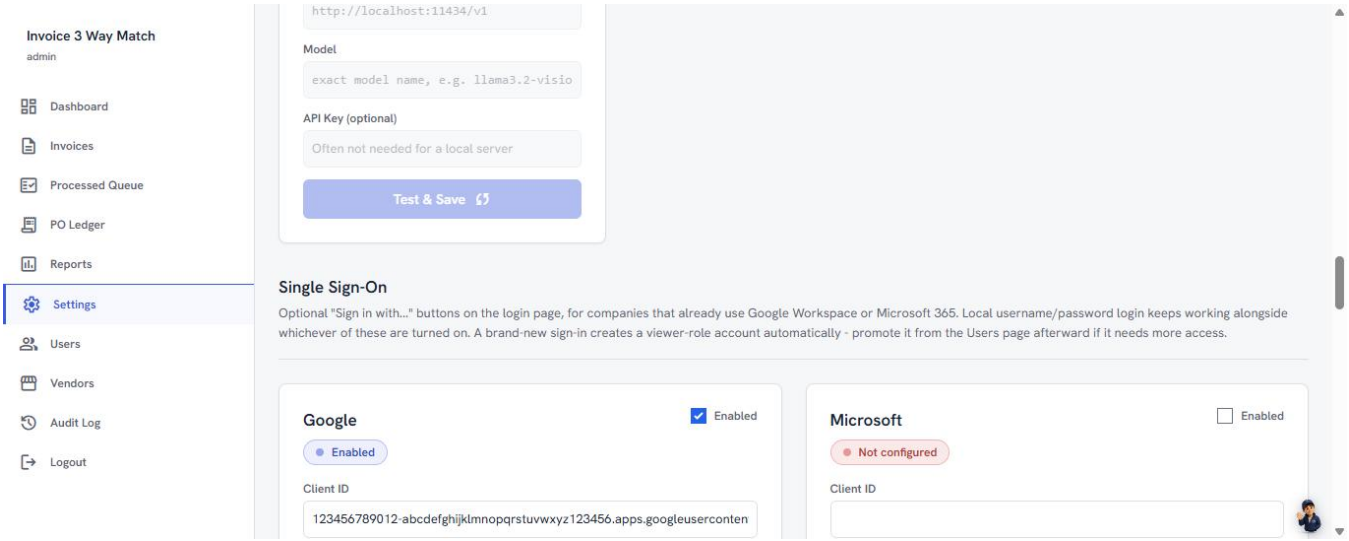
For any of these three, paste the **API Key** from that provider's own developer console and click **Test & Save**. A few things worth knowing about that field:

> **Do:** get your API key from the provider's own website (Google AI Studio, OpenAI's platform, Anthropic's console) — this app never issues or resells one for you.
> **Don't:** expect to see your key again after saving. It's written to this server's own `.env` file, not kept in the browser session, and **never round-trips back to the browser** once saved — the field will just show "Saved - leave blank to keep, or type to replace" from then on. That's deliberate: it's the same reason a saved connector password behaves the same way (see Settings Reference).

Custom (OpenAI-compatible) — for a local or self-hosted model

This option is for keeping invoice data entirely on your own company's network instead of sending it to Google/OpenAI/Anthropic, or for connecting an AI service this app doesn't have a dedicated card for. **This is a genuinely technical setup** — it means running AI software on a computer your company controls, which needs someone comfortable installing server software and typing commands.

If that doesn't describe you or anyone at your company, that's completely fine — just use Google Gemini above instead. Nothing about this option is required; it exists for companies with a specific reason to keep data off the public internet entirely.



Custom (OpenAI-compatible) provider card

Share this box with your IT person or technical colleague — this is what they'll need to set this up.

This card works with any AI server that speaks the widely-supported `/v1/chat/completions` API — Ollama, vLLM, LM Studio, Groq, Mistral, DeepSeek, Together AI, OpenRouter, and Azure OpenAI all qualify. The three fields are:

- **Base URL** — the server's OpenAI-compatible endpoint, including the `/v1` suffix (e.g. `http://localhost:11434/v1` for Ollama running on the same machine as this app).
- **Model** — the exact model name as that server reports it (e.g. `llama3.2-vision` for Ollama). There's no dropdown here, since this could be running anything.
- **API Key (optional)** — most local model servers (Ollama, LM Studio) don't check this; leave it blank unless the server specifically requires one.

Walkthrough for a local Ollama install specifically:

1. Install Ollama on the machine that will run the model, and pull a vision-capable model (invoice extraction needs to read an image/PDF), e.g.:

```
ollama pull llama3.2-vision
```

2. Make sure Ollama is running and reachable from the machine running this app — if they're the same machine, the default `http://localhost:11434` is already correct.
3. In this app's **Settings -> Workspace -> AI Provider**, enable **Custom (OpenAI-compatible)**.
4. **Base URL**: `http://localhost:11434/v1` (the `/v1` is required).
5. **Model**: `llama3.2-vision` (or whichever vision model was pulled).
6. Leave **API Key** blank.
7. Click **Test & Save**.

Pick a model that explicitly supports image/PDF input — a text-only local model can't read an invoice scan at all, and extraction will fail outright.

What switching providers does — and doesn't — do

• Switching is immediate and global: the next invoice extraction (or Help-chat message) uses whichever provider is now active, no restart needed.

• It does **not** re-process anything already extracted — existing invoices in the Processed Queue keep whatever result they got from the provider active at the time.

• The other two cards' saved API keys aren't lost when you switch away from them — they stay configured, just inactive, so you can switch back later without re-entering them.

Where to go next

• Every other Settings screen: Settings Reference

• Getting your first invoice through end-to-end: Approver Guide

Single Sign-On Setup

<- Back to Table of Contents

This entire chapter is optional — everyone can already sign in with a username and password an Admin sets up for them (see Getting Started -> Signing in). Only read this if you specifically want to add a "Sign in with Google" or "Sign in with Microsoft" button as well.

> **This is a technical setup involving Google/Microsoft's own developer consoles — print or share this whole chapter with your IT admin, IT provider, or a technical colleague**, rather than attempting it yourself if that's not a role you're comfortable in. It walks through every click needed, assuming only that whoever does it is comfortable navigating an unfamiliar admin website.
> Looking for the shorter, developer-oriented version instead (environment variables, exact redirect URI format)? See the "Single Sign-On" section in the repository's `SETUP.md`.

What this actually does

Right now, everyone signs in with a username and password an Admin set up for them (see Admin Guide -> Managing users). SSO adds an **alternative, optional** way in: a "Sign in with Google" and/or "Sign in with Microsoft" button on the login screen, so your team can use the same company Google/Microsoft account they already use for email instead of remembering another password.

A few things worth knowing up front:

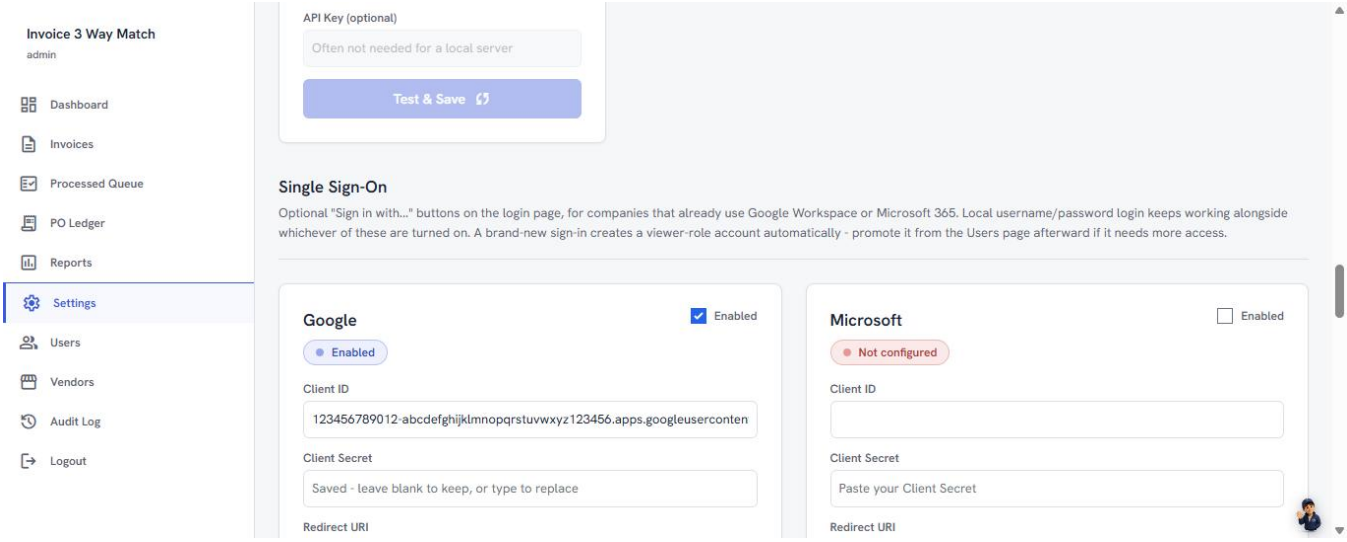
- **This is additive, not a replacement.** Existing username/password logins keep working exactly as before. You can turn SSO on for some people and leave others on local login.
- **You need your own Google or Microsoft account for this**, not this app's. Each company that uses this app connects their *own* Google Cloud / Azure account — nothing is shared between different companies using this software, and nothing about your setup is visible to anyone else.
- **The first time someone signs in with Google/Microsoft, a new account is created for them automatically** — with the lowest access level (Viewer). You then promote them to Approver or Admin from the Users page if they need more access. Nobody gets more access than the minimum just by signing in.
- There are two separate setups below — Google and Microsoft — do either one, or both. They don't depend on each other.

Before you start: get the Redirect URI from this app

Both Google and Microsoft will ask you for a "Redirect URI" — a web address they send people back to after they sign in. **Get this from the app itself, not from this chapter** — it depends on exactly how your copy of this app is set up (its own web address), so a value copied from a document would be wrong.

1. Log into this app as an Admin.

2. Go to **Settings -> Workspace -> Single Sign-On**. You'll see a card for Google and a card for Microsoft, each showing its own **Redirect URI**:



Single Sign-On cards, Google and Microsoft

3. Keep this page open in a tab — you'll come back to copy each Redirect URI and to paste in the Client ID/Secret you get below.

Part 1: Google

Step 1 — Create a Google Cloud project

1. Go to the Google Cloud Console.

2. Sign in with the Google account that manages your company's Google Workspace (or any Google account, if you're not using Workspace).

3. At the top of the page, click the project dropdown and choose **New Project**. Give it a name like "Company Name — App Login" and click **Create**. It takes a few seconds.

4. Make sure the new project is selected (check the dropdown at the top again) before continuing.

Step 2 — Configure the "OAuth consent screen"

This is the screen your team will briefly see when they click "Sign in with Google" — it also controls who is *allowed* to sign in at all.

1. In the left-hand menu, go to **APIs & Services -> OAuth consent screen**.

2. **User Type** — the single most important choice on this whole page:

   • **Internal** — pick this if your company uses **Google Workspace** (i.e., your staff's email addresses are on your own company domain, managed centrally). Strongly recommended when available: sign-in works immediately for everyone in your organization, with no review process, no warning

screens, and no user limit.

- **External** — pick this if your team signs in with regular personal Gmail addresses (no

Google Workspace), or "Internal" isn't offered to you. This works too, but see **Testing vs. Production** below — it has a couple of extra steps and a temporary limitation.

3. Fill in the required fields: App name (e.g., your company name), User support email, and

Developer contact email. You can skip optional fields like a logo.

4. On the "Scopes" step, you don't need to add anything — this app only ever asks for a

person's name and email address (the built-in `openid` and `email` scopes), which doesn't require any extra scope configuration or Google's app-review process.

5. Save and continue through to the end of the wizard.

If you chose External — the "Testing vs. Production" distinction that matters:

A brand-new External app starts in **Testing** mode. In this mode, **only people you've explicitly added as a "test user" can sign in** — anyone else clicking "Sign in with Google" will see an error, not a login screen. There's a limit of 100 test users.

- To add people: on the OAuth consent screen page, find the **Test users** section, click

Add users, and enter the Google email address of each person who should be able to sign in. This takes effect within a minute or two.

- When you're ready for **anyone** to be able to sign in (not just people on that list), come

back to this page and click **Publish App** to move it to Production. Because this app only requests basic `openid`/`email` scopes, this does **not** require Google's formal verification review — but people signing in for the first time may briefly see an "unverified app" warning screen with a "Continue" link before reaching the sign-in page. This is normal and expected for a small internal business tool; it goes away once/if you complete Google's optional verification process, which isn't necessary for most companies using this privately.

If you chose **Internal**, none of the above applies — skip straight to Step 3.

Step 3 — Create the OAuth Client ID

1. In the left-hand menu, go to **APIs & Services -> Credentials**.
2. Click **+ Create Credentials -> OAuth client ID**.
3. **Application type**: choose **Web application**.
4. Give it a name (e.g., "3-Way Match Login").
5. Under **Authorized redirect URIs**, click **+ Add URI** and paste the exact **Google**

Redirect URI you copied from this app's Settings page earlier. It must match exactly, including `http` vs `https` — a common mistake is a trailing slash or the wrong protocol.

6. Click **Create**. A popup shows your **Client ID** and **Client Secret** — copy both

somewhere safe for a moment. You can always come back and view the Client ID later, but Google only shows the full secret once at creation time (though you can generate a new one later if you lose it).

Step 4 — Connect it in this app

1. Back in this app's **Settings -> Workspace -> Single Sign-On**, paste the **Client ID** and **Client Secret** into the Google card.
2. Turn the **Enabled** switch on for Google.
3. Click **Save**.

> **Do:** test it for real by clicking "Sign in with Google" on the login page — there's no "Test Connection" button for SSO, since proving it actually works requires a real browser signing in through Google's own screen.

Part 2: Microsoft

Step 1 — Register an app in Azure

1. Go to the Azure Portal and sign in with your Microsoft 365 admin account (or any Microsoft account).
2. Search for and open **Azure Active Directory** (sometimes shown as **Microsoft Entra ID**).
3. In the left-hand menu, go to **App registrations -> New registration**.
4. Give it a name (e.g., "3-Way Match Login").
5. Under **Supported account types**, choose **"Accounts in any organizational directory and personal Microsoft accounts"**. This specific option is required — this app is built to work with either a Microsoft 365 organization or a personal Microsoft account without needing to know which one in advance, and it won't work correctly if a narrower option is chosen here.
6. Under **Redirect URI**, choose platform **Web**, and paste the exact **Microsoft** Redirect URI you copied from this app's Settings page. Then click **Register**.

Step 2 — Create a Client Secret

1. On your new app's page, go to **Certificates & secrets** in the left-hand menu.
2. Under **Client secrets**, click **+ New client secret**. Give it a description (e.g., "App login") and choose an expiry (Microsoft's longest built-in option, e.g. 24 months, is usually the simplest choice).
3. Click **Add**. **Immediately copy the secret's "Value" column** — this is the only time Microsoft shows it in full; if you navigate away without copying it, you'll need to create a new one.

> **Don't** forget: unlike Google, every Microsoft client secret has an expiration date you chose above. When it expires, Microsoft sign-in will stop working with an authentication error until someone creates a new secret and updates it here. Put a reminder on your calendar a few weeks before the expiry date you picked.

Step 3 — Get the Client ID

1. Go back to **Overview** for your app registration.
2. Copy the **Application (client) ID** shown there.

Step 4 — Connect it in this app

1. In this app's **Settings -> Workspace -> Single Sign-On**, paste the **Application (client)

ID **and the** Client Secret value** you copied into the Microsoft card.

2. Turn the **Enabled** switch on for Microsoft.
3. Click **Save**.

As with Google, test it for real by clicking "Sign in with Microsoft" on the login page rather than relying on a "Test" button — there isn't one, for the same reason.

How sign-in actually behaves

• **First-time sign-in**: a brand-new account is created automatically, using the person's

email address as their username, with the **Viewer** role (read-only access everywhere — see the Viewer Guide). An Admin then promotes them from the Users page if they need to approve invoices, manage settings, etc.

• **Matching an existing account**: if you'd rather have someone's Google/Microsoft sign-in go

straight into an account you've already set up (with whatever role you gave it) rather than create a new Viewer account, create that user first from the Users page with **their email address as the username**. The match is case-insensitive.

• **Local login keeps working**: anyone with a username/password can still use it, whether or

not SSO is turned on. See Getting Started -> Signing in.

Troubleshooting

What you see	Likely cause	Fix
"redirect_uri_mismatch" (Google) or an AADSTS error about a reply URL (Microsoft)	The redirect URI in the provider's console doesn't exactly match what this app expects	Re-copy the Redirect URI from this app's Settings page and compare character-for-character with what's registered in Google Cloud Console / Azure — check for `http` vs `https` and a trailing slash
Google shows "Google hasn't verified this app"	Expected in Testing mode, or right after Publishing an External app (see Part 1, Step 2)	If it's a person you added as a test user, this warning is normal — they click "Continue" (may be behind an "Advanced" link) to proceed. If it's someone NOT on the test user list, add them, or publish the app
"Error 403: access_denied" on Google	The signed-in Google account isn't on the Test users list yet	Add that email under OAuth consent screen -> Test users, or publish the app

What you see	Likely cause	Fix
Microsoft sign-in suddenly stops working for everyone	The client secret expired (see Part 2, Step 2)	Create a new client secret in Azure, update it in this app's Settings
Microsoft sign-in fails immediately with an error mentioning the account type or tenant isn't supported	The app registration's account type was set too narrowly	In Azure, the account type must be "Accounts in any organizational directory and personal Microsoft accounts" — this can only be changed by re-registering the app, it's not editable after creation
"That Google/Microsoft email address isn't verified yet"	The person's email isn't verified with that provider	They need to verify their email address directly with Google/Microsoft first, then try again
Sign-in succeeds but lands on a read-only/limited view	This is the intended behavior for a brand-new auto-provisioned account (Viewer role)	An Admin promotes their role from the Users page

Keeping this secure

Do: treat the **Client Secret** for either provider exactly like a password — anyone who has it could impersonate your app's login flow. Only paste it into this app's Settings; never share it elsewhere.
Do: if a secret is ever exposed or you're unsure, generate a new one in Google Cloud Console / Azure Portal and update it in this app's Settings immediately — the old one keeps working until you explicitly delete/revoke it there, so do that too once the new one is confirmed working.
Don't give more people access to your Google Cloud / Azure admin console than need it — that access is separate from (and more powerful than) anyone's role inside this app.

Where to go next

- Every other Settings screen: Settings Reference
- Creating and promoting user accounts: Admin Guide -> Managing users