real world technology solutions

CLIENT ADMINISTRATOR GUIDE

# Fax Client

Managing your users, sending identities, fax-number delivery, and security for your organisation.

AUTHOR
**Real World Technology Solutions**

DATE
**August 2026**

real world technology solutions

# Contents

real world technology solutions

## Signing in

Open your Fax Client web app and sign in with your email and password.

1. Go to your Fax Client address in a web browser (for example, `https://faxclient.rwts.com.au`). The sign-in page appears.

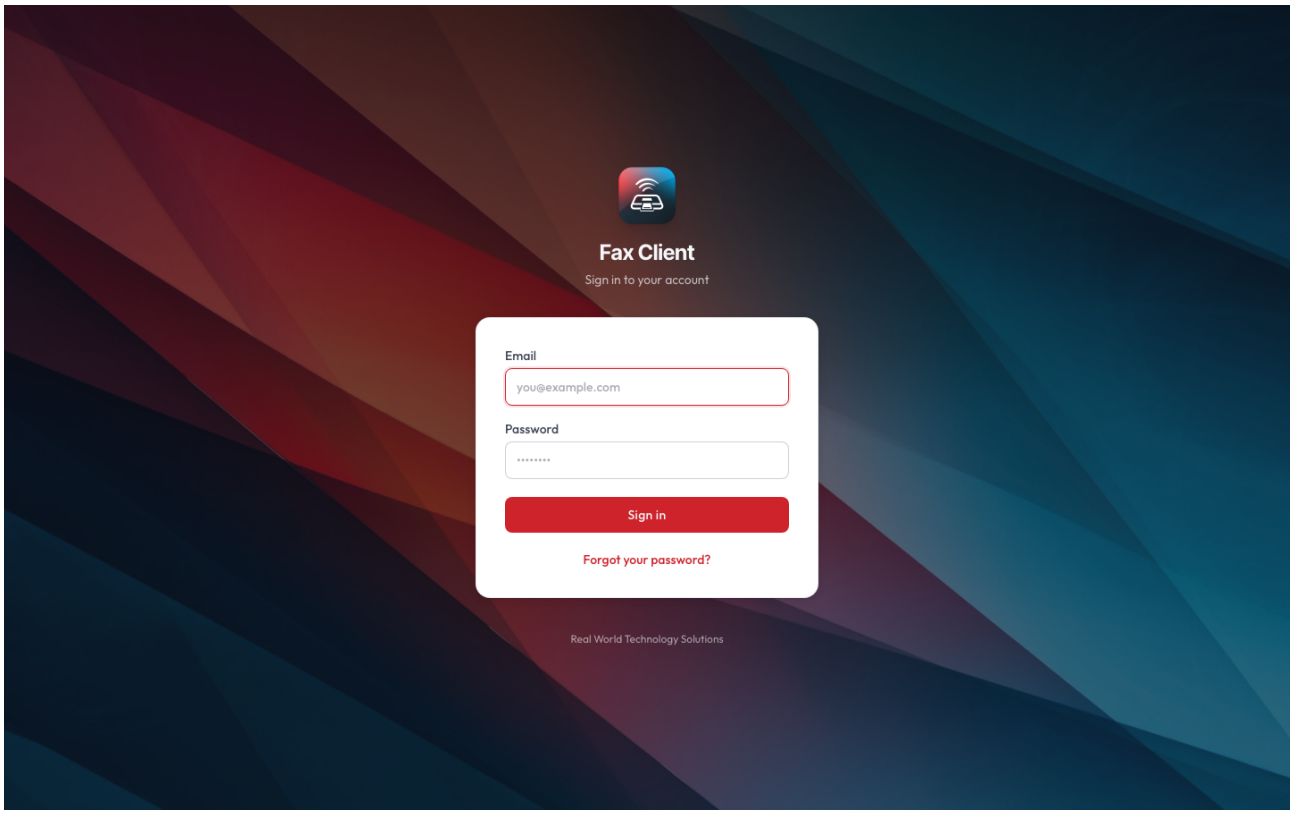


Figure 1: The Fax Client sign-in page

2. Enter your email and password.
3. Click the sign-in button.
4. If two-factor authentication is enabled on your account, you are then asked for the 6-digit code from your authenticator app. See the Two-factor authentication topic for details.

After signing in, you land on your home page. For fax senders, this is the Outbox.

The top header contains the navigation, a help (**?**) button, a light/dark theme toggle, your email address, and a **Sign out** button.

If you have forgotten your password, use the **Forgot password** link on the sign-in page.

# Two-factor authentication

Two-factor authentication (2FA) adds a second check to your sign-in, so a password alone is not enough to access your account.

## Turn on 2FA

1. Go to **Settings** and find the **Two-factor authentication** section.

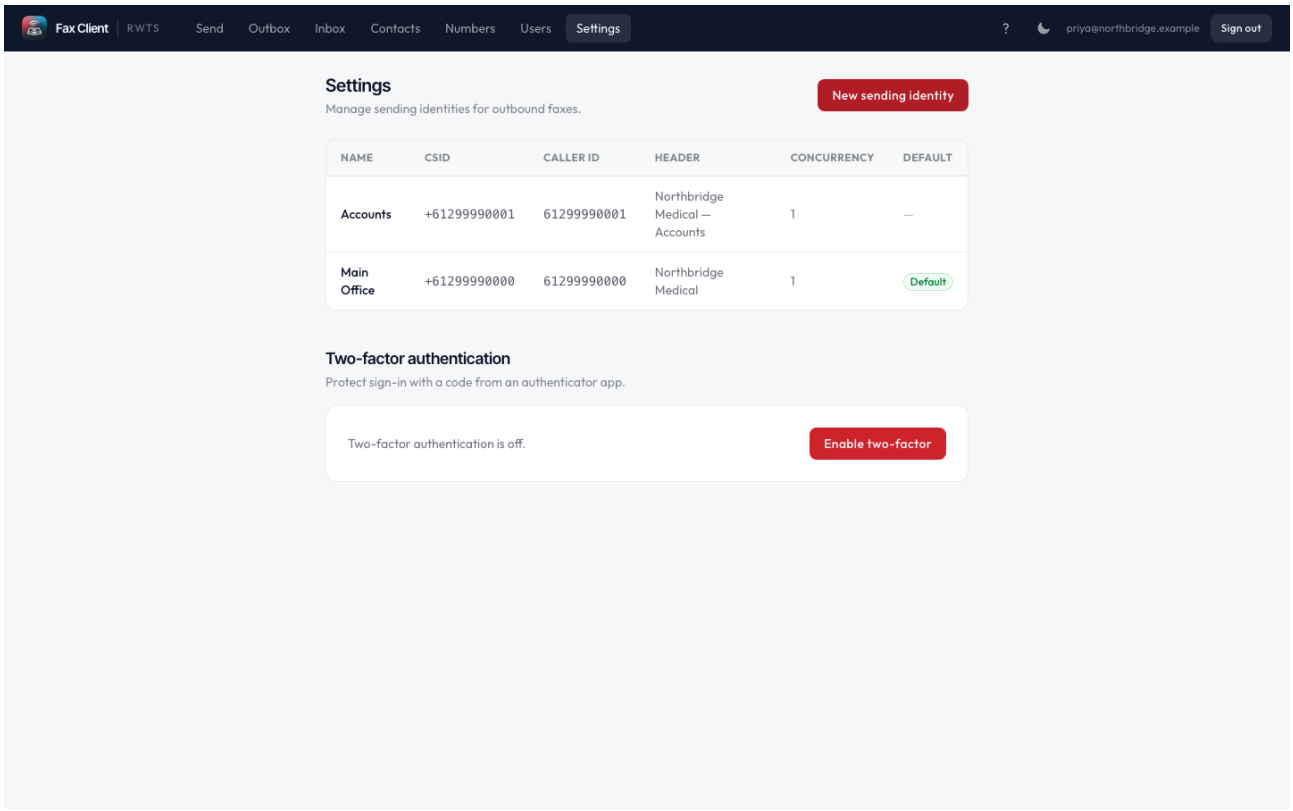


Figure 2: The Two-factor authentication section on the Settings page

2. Click **Enable**.
3. Scan the QR code with an authenticator app (such as Google Authenticator, Microsoft Authenticator, or 1Password).
4. Enter the 6-digit code your authenticator app shows to confirm.
5. You'll be shown one-time backup codes. Save these somewhere safe. Each code can be used once if you can't reach your authenticator app.

## Signing in with 2FA

The next time you sign in, after your password you'll be asked for the current 6-digit code from your authenticator app.

## Turn off 2FA

1. Go to **Settings** and find the **Two-factor authentication** section.
2. Click **Disable**.
3. Enter a current 6-digit code to confirm.

## If your organisation requires 2FA

Your organisation's administrator may require 2FA. If so, you'll be prompted to set it up before you can use the app.

# Resetting your password

If you have forgotten your password, you can request a reset link from the sign-in page.

1. On the sign-in page, click **Forgot password**.

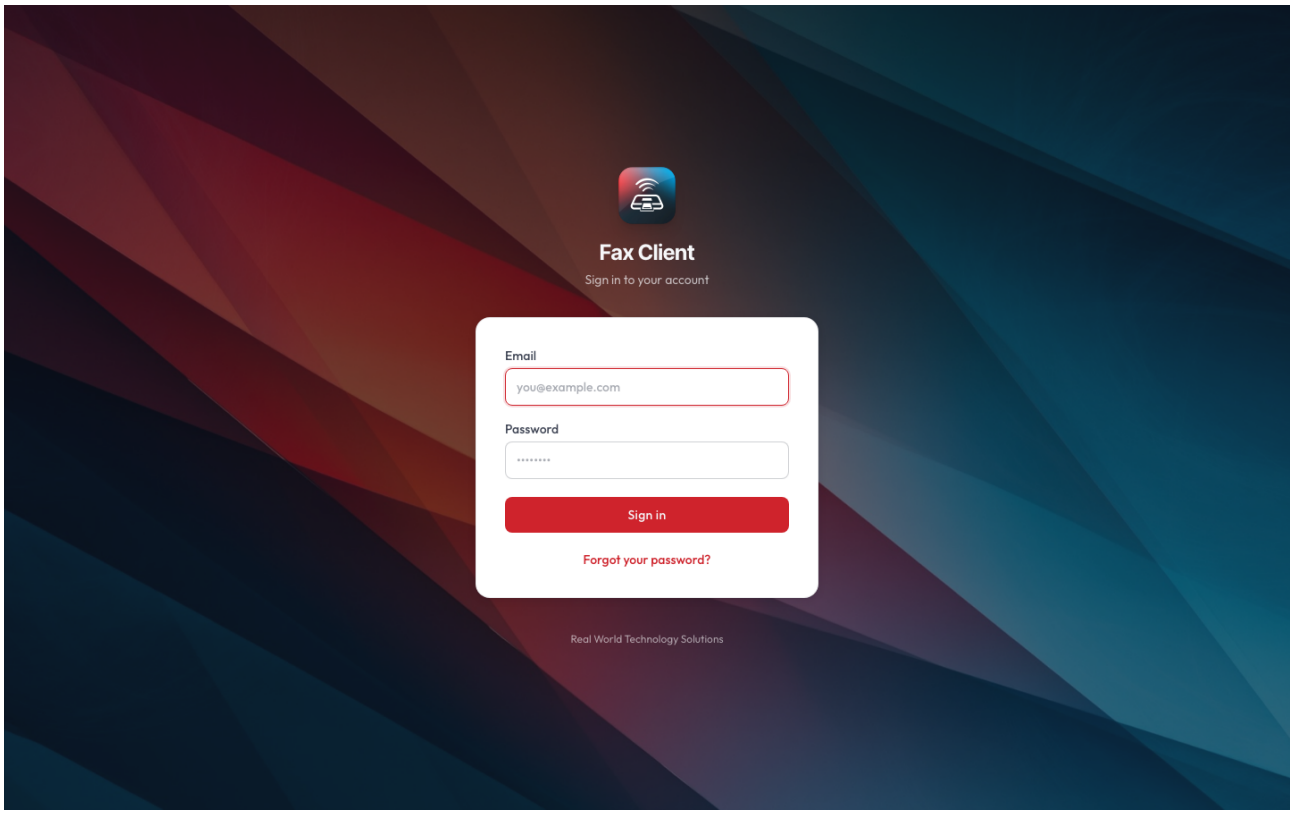


Figure 3: The sign-in page, showing the Forgot password link

2. Enter your email address and submit the form. If that address belongs to an account, a reset link is emailed to you. The response looks the same whether or not an account exists.
3. Open the email and follow the reset link, then choose a new password. The link is single-use and expires after a short time, so complete this step promptly.
4. Setting a new password signs you out everywhere. Sign in again with your new password.

New users receive the same kind of link from an invitation email. Use it to set your first password before it expires.

# Getting help

The help panel is built into the app and available on every page.

1. Click the **?** button in the top header to open the help panel.

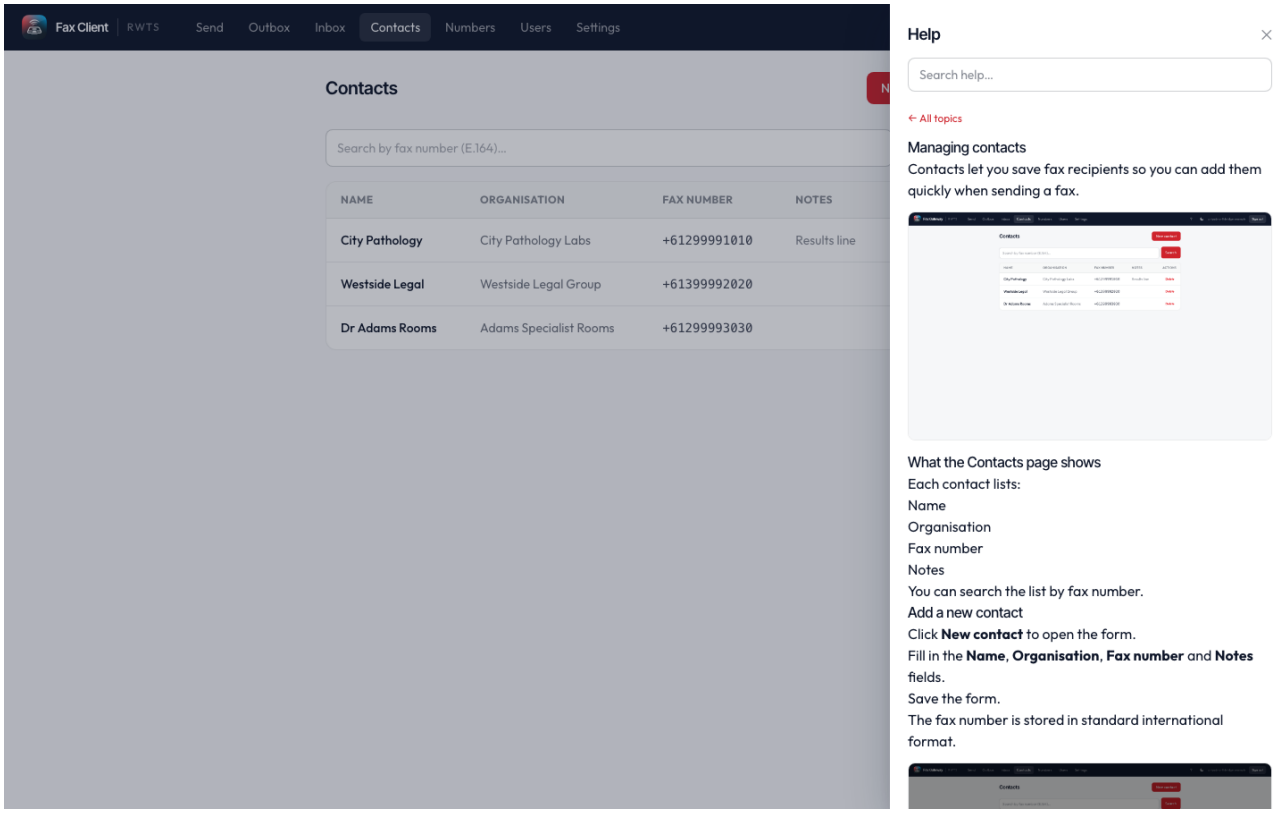


Figure 4: The help panel showing contextual topics and a search field

2. The panel shows the topics relevant to the page you are on first.
3. To find something specific, type a keyword into the search field to search all topics.

## Other ways to get help

- The same guides are available as downloadable PDFs from RWTS or your provider.
- For anything not covered, contact your administrator.
- If your administrator cannot help, contact RWTS support or your white-label provider's support team.

# Sending a fax

Open the **Send** page from the top navigation to send a fax to one or more recipients.

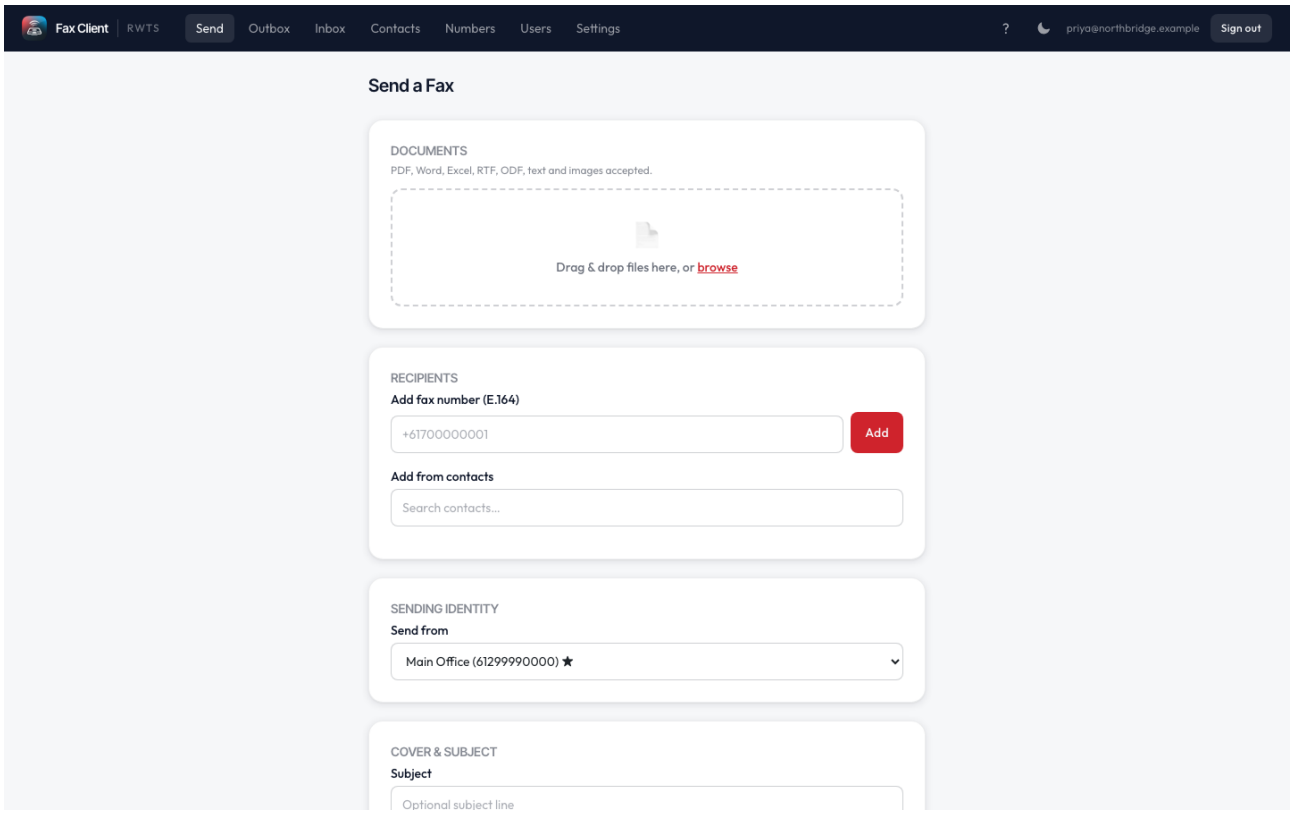


Figure 5: The Send page, showing the document upload area, recipient field, sending identity selector and cover page options

## Steps

1. Open **Send** from the top navigation.
2. Add your documents by dragging files onto the upload area, or click it to choose files. Documents are sent in the order you add them, up to 20 per fax.
3. Add recipients by typing a fax number directly in international format (for example, +61 2 9999 0001), or search your saved contacts and click a contact to add them. You can add more than one recipient.
4. Choose a **Sending identity** — the fax line your fax is sent from. Your default is pre-selected.
5. To include a cover page, tick **Include cover page** and add a **Subject** and a cover note. The cover page is added as the first page of your fax.
6. Click **Send**. You're taken to the fax's detail page, where you can watch its progress.

real world technology solutions

## Before you can send

You need all three of the following:

- At least one document
- At least one recipient
- A sending identity selected

## Supported file types

- PDF
- Word
- Excel
- RTF
- OpenDocument
- Plain text
- Images

You can add up to 20 documents per fax.

# Tracking sent faxes (the Outbox)

The Outbox is your home page and lists the faxes you've sent.

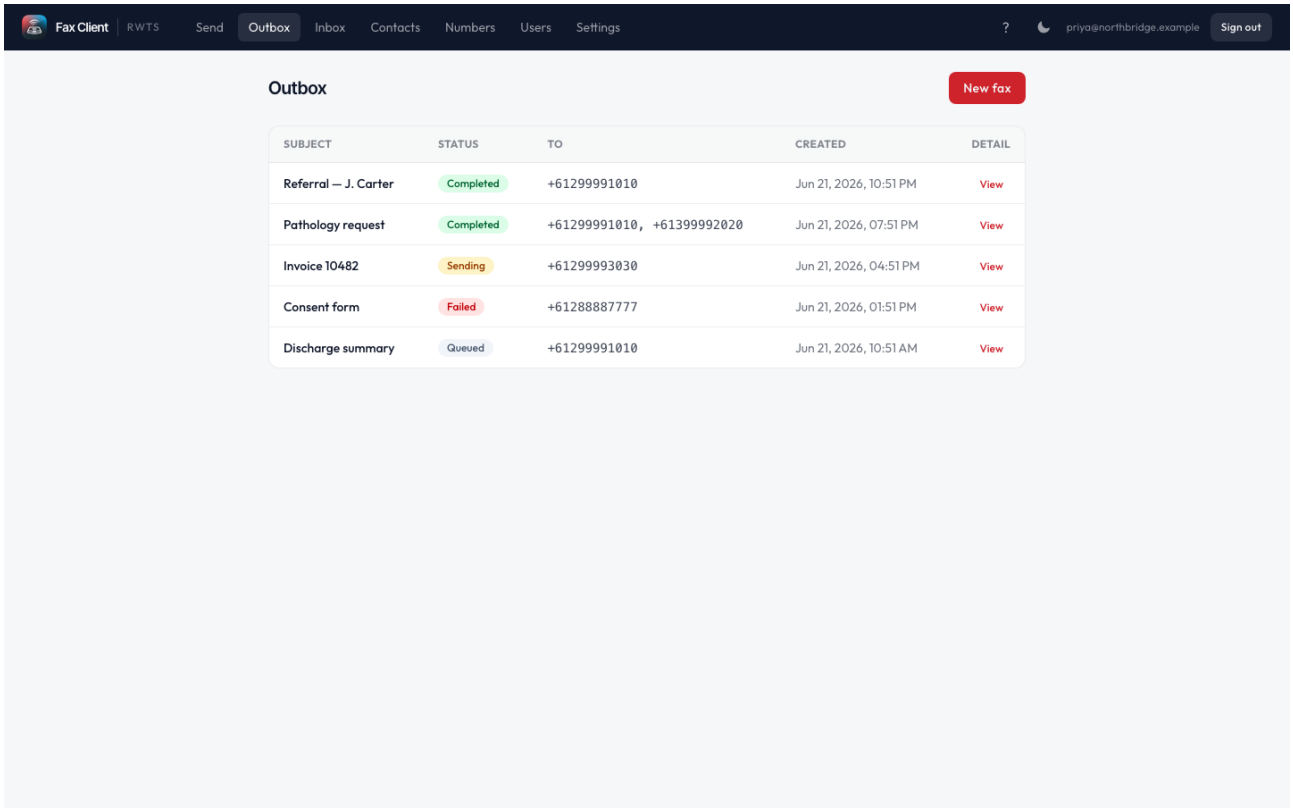


Figure 6: The Outbox listing sent faxes with their subject, status, recipients and creation time

## What you'll see

- Each row shows the **Subject**, the current status, the recipients, and when the fax was created.
- The list updates on its own while a fax is still in progress — you don't need to reload the page.
- It stops updating once the fax reaches a final status.

## Statuses

- **Queued** — the fax is waiting to be processed.
- **Converting** — your documents are being prepared.
- **Ready** — the fax is ready to send.
- **Sending** — transmission is in progress.
- **Completed** — every recipient has finished.
- **Failed** — the fax could not be prepared or sent.

For a fax to several recipients, the status shows **Completed** only once all recipients have finished. Open the fax to see the result for each recipient.

## Common tasks

1. To send a new fax, click **New fax**.
2. To see the detail for a sent fax, including each recipient's result, open its row in the list.

# Fax details, previews and retrying

Open any fax from your **Outbox** to see a full breakdown of how it went.

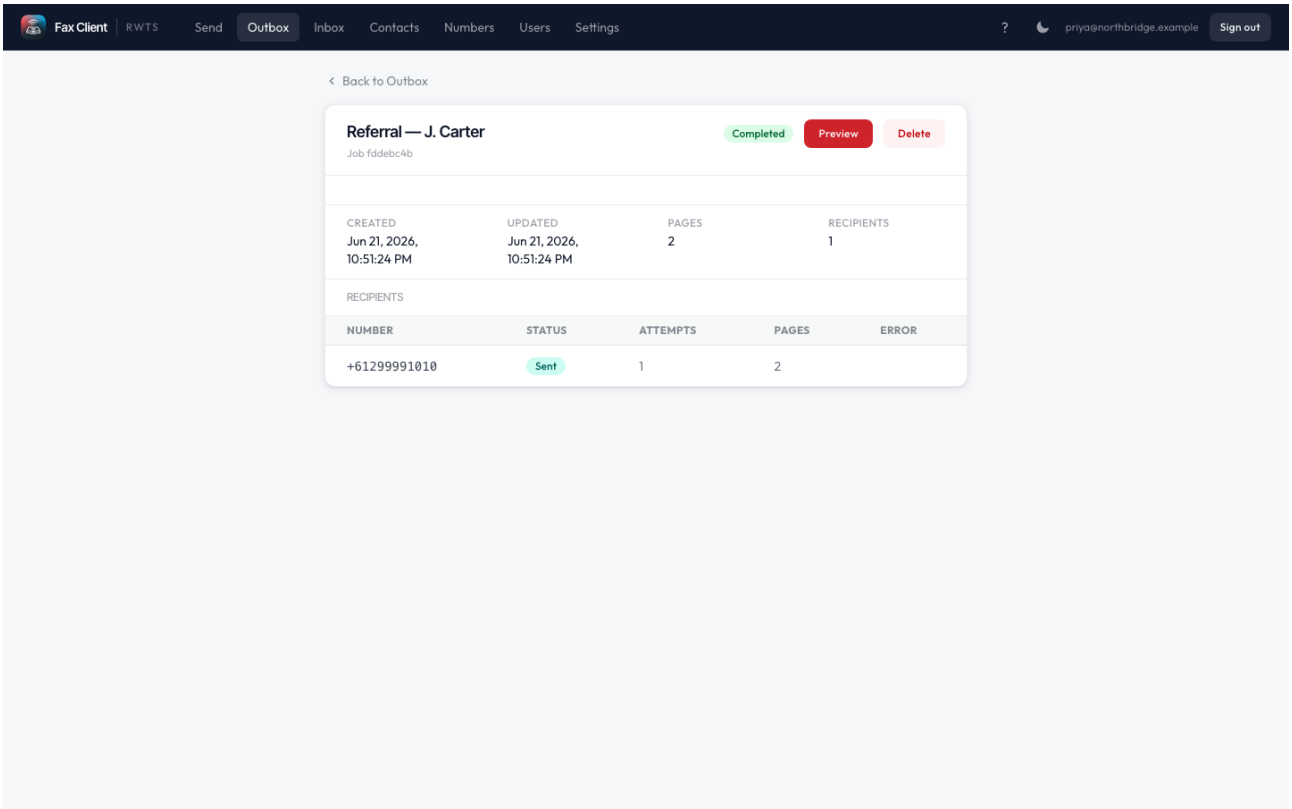


Figure 7: The fax detail page, showing job status, the recipient table and the available actions

## What the detail page shows

- The overall status of the fax
- The page count
- When the fax was created and last updated
- A table of every recipient, each with its own status (**Sent**, **Sending**, **Queued** or **Failed**) and any error

## Preview the fax

1. Open the fax from your **Outbox**.
2. Select **Preview**. The exact pages that were faxed open as a PDF in your browser.

## Retry failed recipients

If one or more recipients failed, you can re-send to just those recipients.

1. Open the fax from your **Outbox**.

2. Select **Retry**. The fax is re-sent only to recipients with a **Failed** status. Recipients already marked **Sent** are left alone.

### Delete a fax

1. Open the fax from your **Outbox**.
2. Select **Delete**. The fax is removed from your list.

Deleting is a soft delete, so the fax is recoverable for a period afterwards. After that window it is permanently purged, according to your organisation's retention setting.

# Managing contacts

Contacts let you save fax recipients so you can add them quickly when sending a fax.

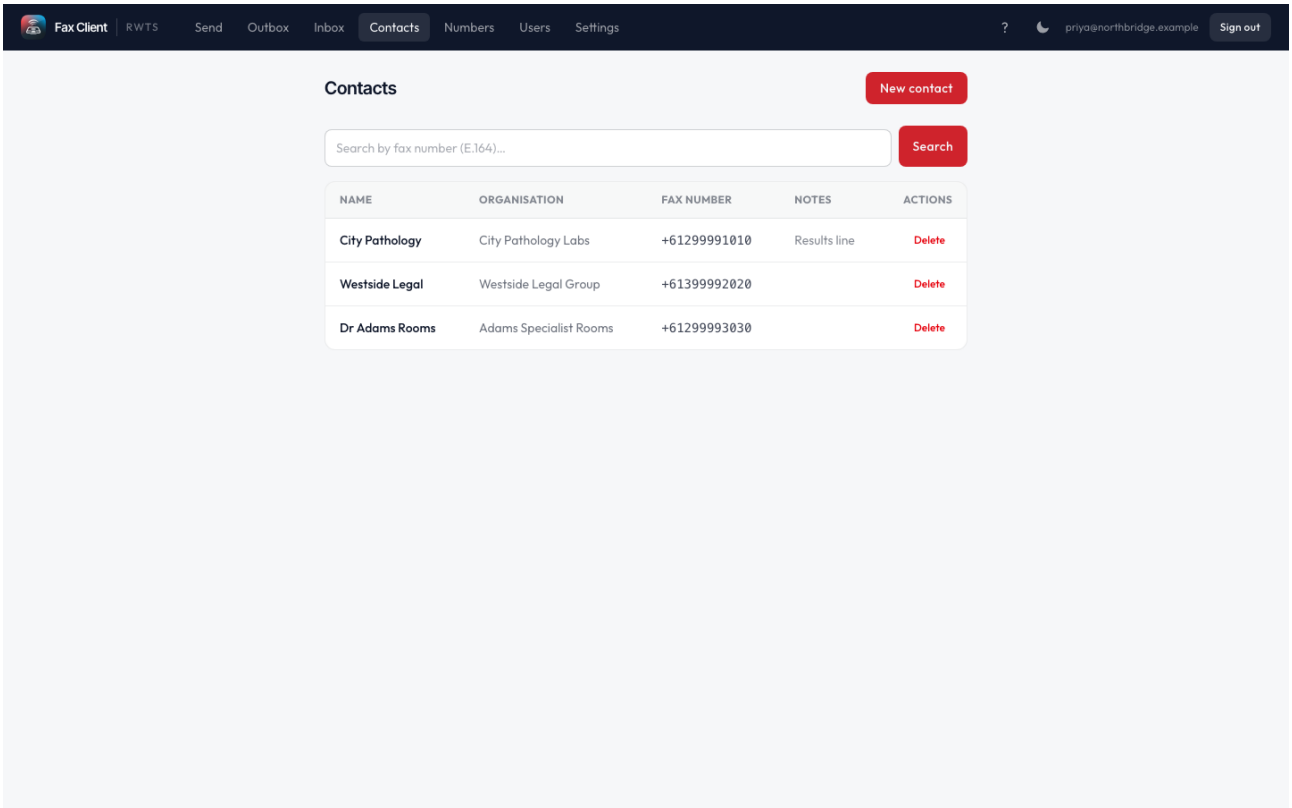


Figure 8: The Contacts page listing saved recipients by name, organisation, fax number and notes

## What the Contacts page shows

Each contact lists:

- Name
- Organisation
- Fax number
- Notes

You can search the list by fax number.

## Add a new contact

1. Click **New contact** to open the form.
2. Fill in the **Name**, **Organisation**, **Fax number** and **Notes** fields.
3. Save the form.

The fax number is stored in standard international format.

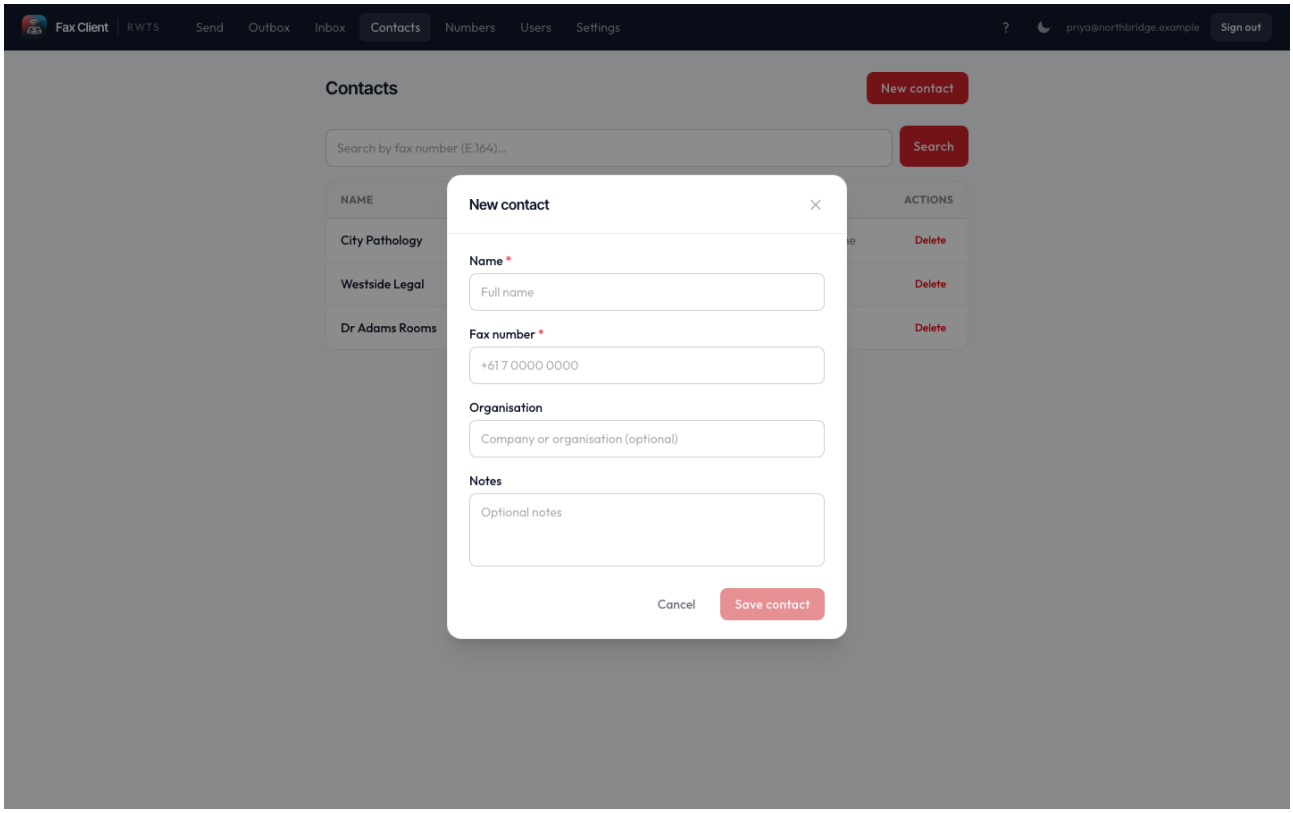


Figure 9: The New contact form with fields for Name, Organisation, Fax number and Notes

### Delete a contact

Delete a contact from its row on the Contacts page.

### Using contacts when sending

Your contacts appear in the recipient search on the Send page, so you can add a recipient with a single click instead of typing the fax number.

### Shared across your organisation

Contacts are shared across everyone in your organisation.

# Receiving faxes

Inbound faxes are emailed to you as PDFs and can also be viewed in the Inbox.

## How faxes are delivered

Faxes are received on your organisation's fax number(s). When one arrives, it is converted to a PDF and emailed to the delivery addresses configured for that number. Each recipient gets their own copy.

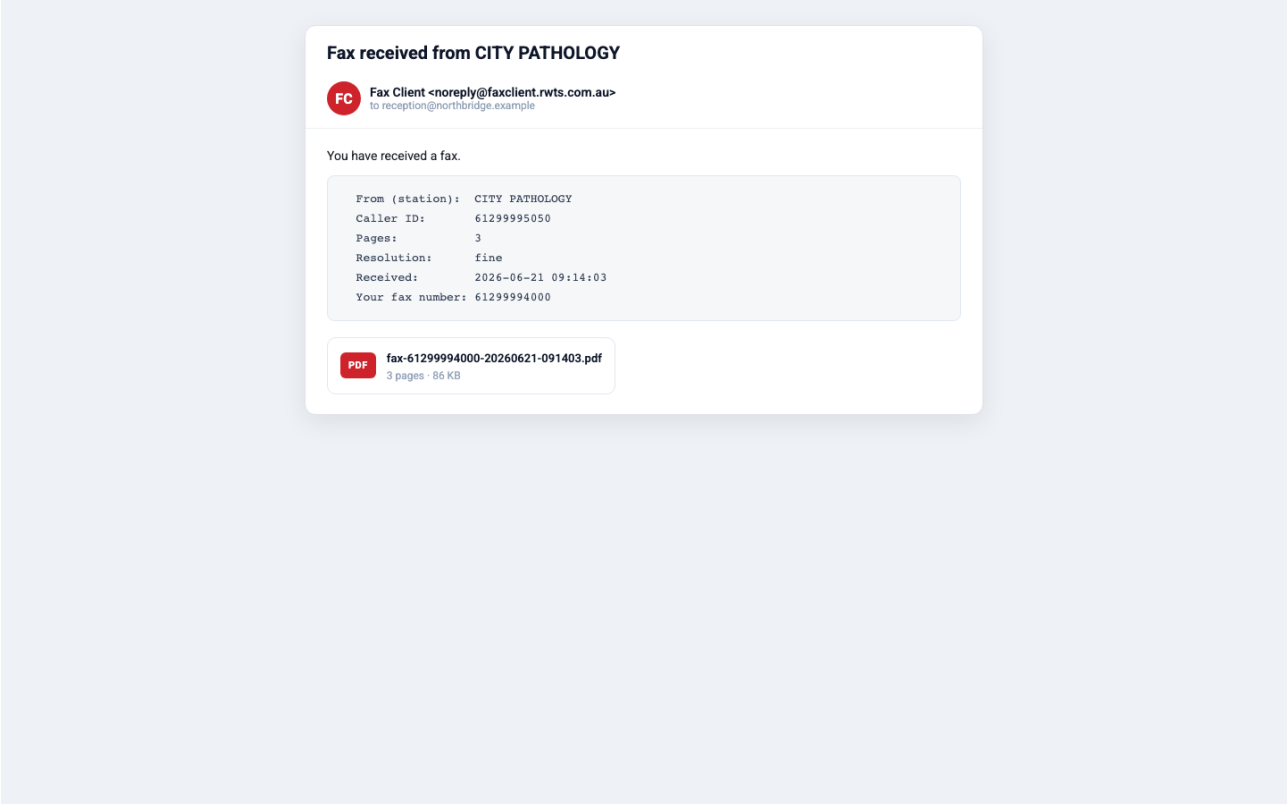


Figure 10: Delivery email for a received fax, showing the sender, pages and received details with the PDF attached

The delivery email includes:

- The subject **Fax received from <station>**
- The sender, page count and received time
- The fax as an attached PDF

## Viewing faxes in the Inbox

You can also see received faxes in the **Inbox**.

1. Open the **Inbox**.

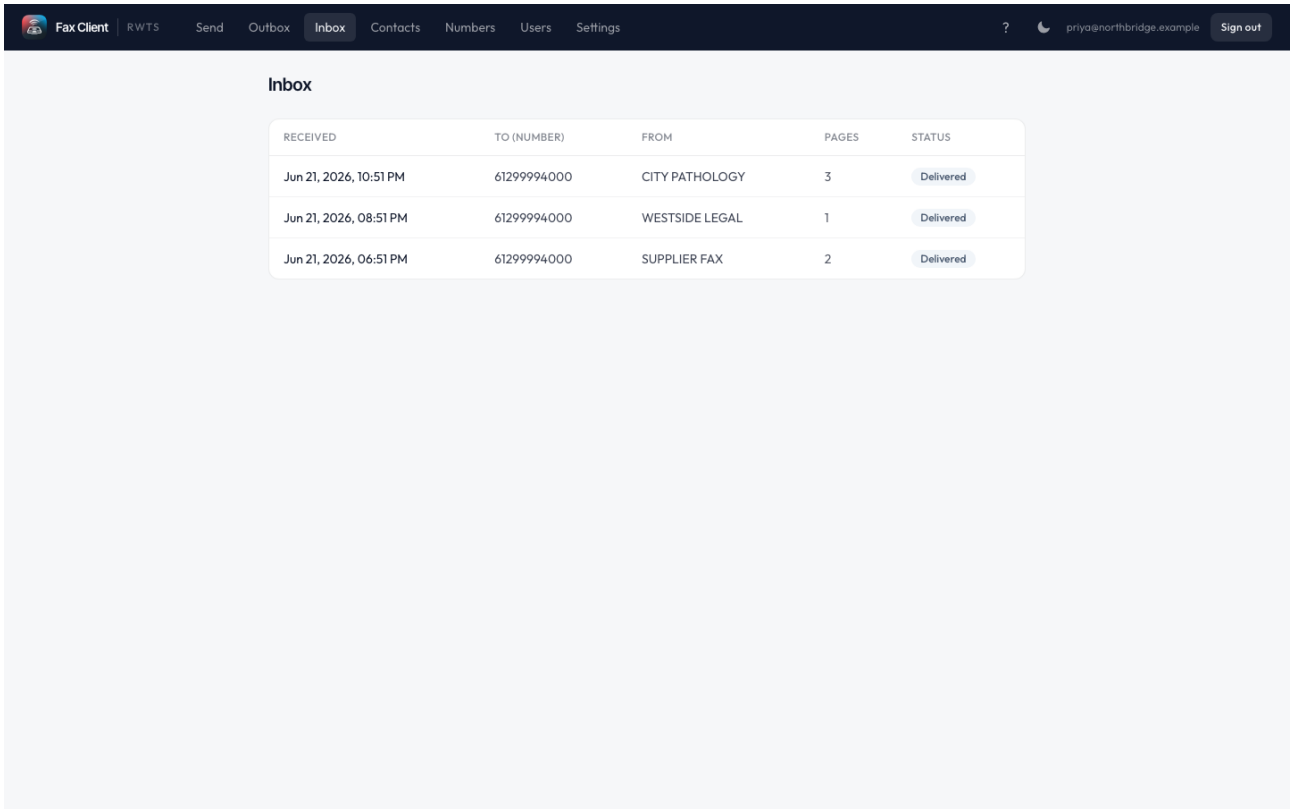


Figure 11: Inbox listing received faxes with received time, number, sender, pages and status

The Inbox shows each fax's received time, the number it came in on, who it is from, the page count and the status.

2. Open a fax to view its details.

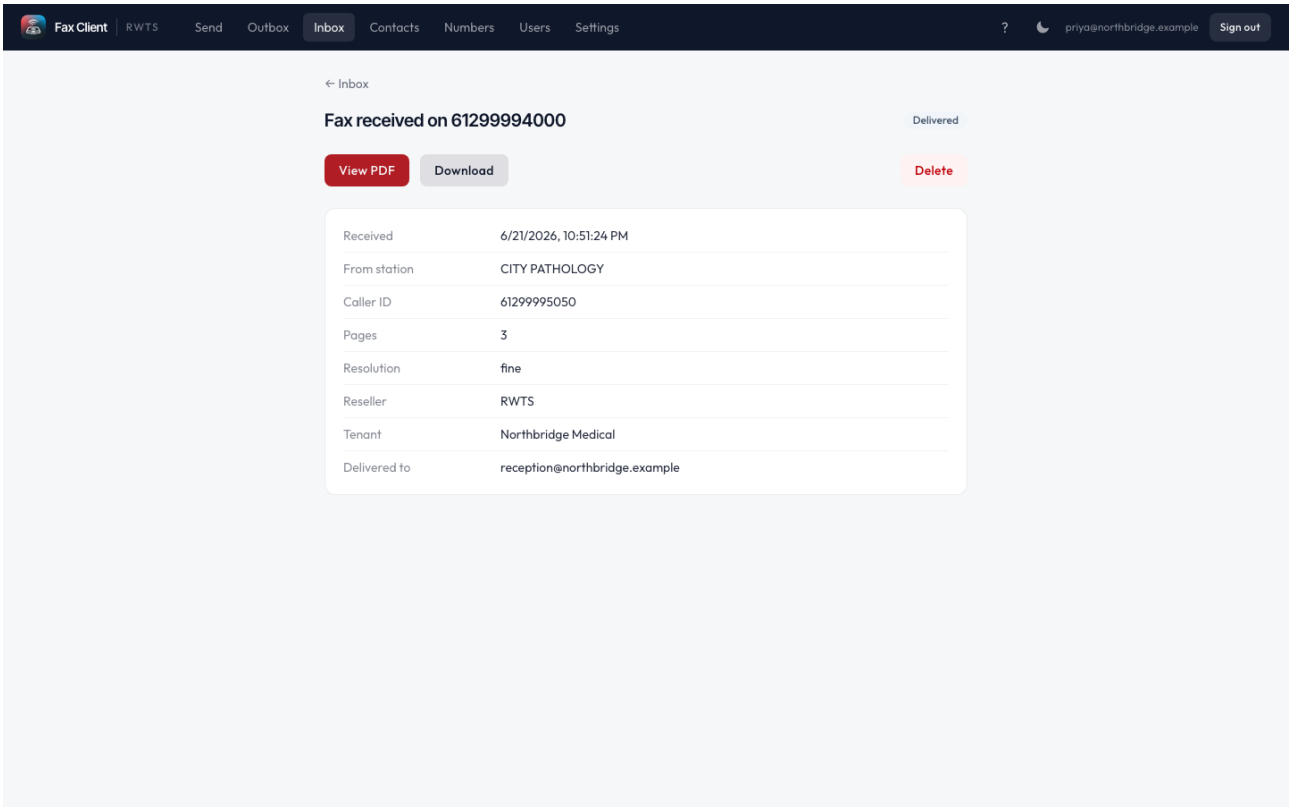


Figure 12: Received fax detail showing the fax details with options to view, download or delete

3. From the detail view you can view or download the PDF, see the details, or delete the fax.

## Who sets the delivery addresses

A tenant administrator sets which email addresses receive each number's faxes. See the Fax-number delivery topic for details.

# Sending a fax by email

If your administrator has enabled email-to-fax for your organisation, you can send a fax directly from your email client.

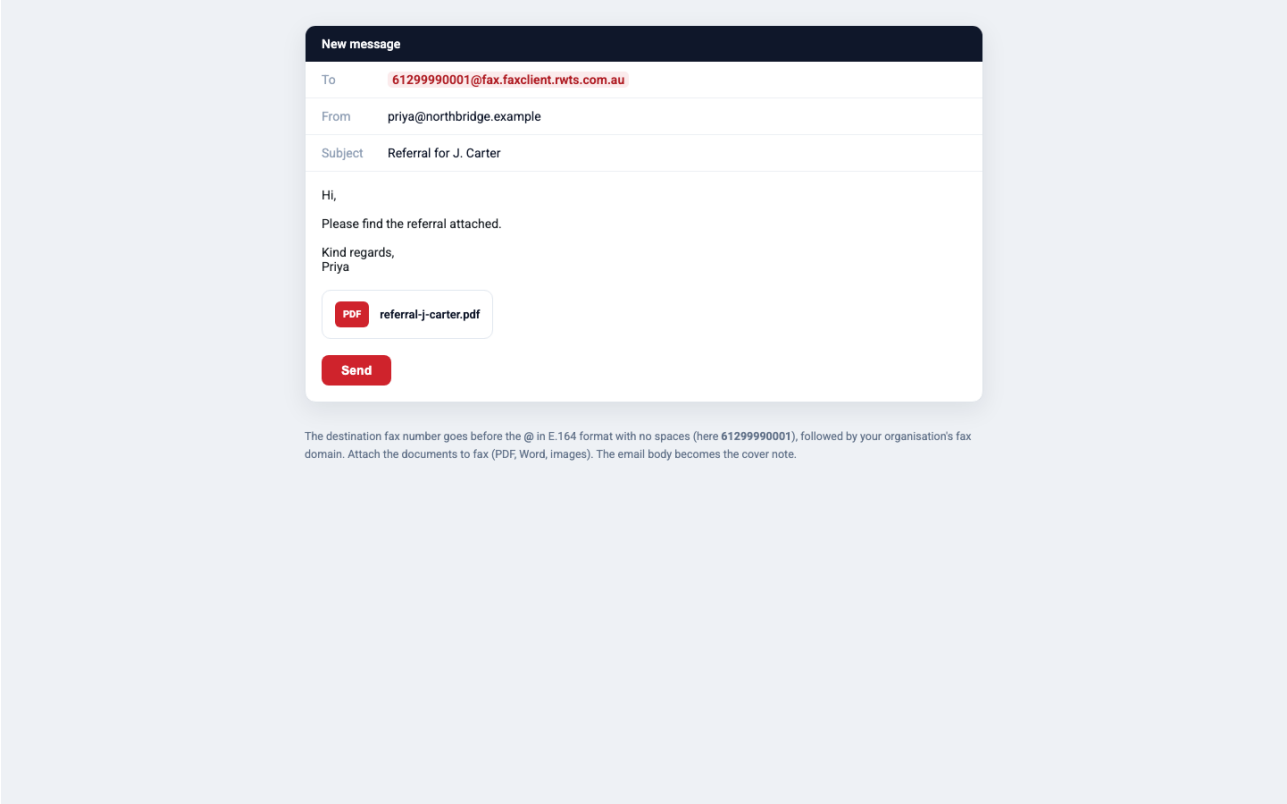


Figure 13: The email-to-fax feature in Fax Client, enabled for your organisation

## How to send

1. Create a new email in your email client.
2. In the **To** field, enter the fax number followed by your fax domain — for example, `61299990001@fax.faxclient.rwts.com.au`. The fax number must be in international format with no spaces or plus sign (`+`). Your administrator will give you the exact domain to use.
3. Add a **Subject** and body text if you want a cover note — both become the cover note on the fax.
4. Attach the documents you want to fax (PDF, Word, or image files).
5. Send the email.

If the fax cannot be sent, you will receive an email back with the reason.

## Things to know

- Email-to-fax must be turned on by your administrator before you can use it.

- Only approved sender addresses or domains are permitted to send faxes this way.
- Your email must pass standard email authentication (DMARC) — emails that fail authentication will not be sent.
- Your administrator provides the fax domain for your organisation.

real world technology solutions

# Administrator overview

As an administrator for your organisation, you manage everything from within the web app — there is no separate admin site to log into. Everything you manage is scoped to your own organisation.

## What you can do

- **Users** — add and manage the people in your organisation.
- **Settings** — manage your sending identities and fax lines.
- **Numbers** — choose who receives faxes on your fax numbers.
- Require two-factor authentication.

## Fax numbers and plans

You manage the delivery of the fax numbers you already have. New fax numbers, and changes to your plan, are arranged through RWTS or your provider — contact them directly for those requests.

# Managing users

The Users page shows everyone in your organisation and lets you invite new people, change their role, or remove access.

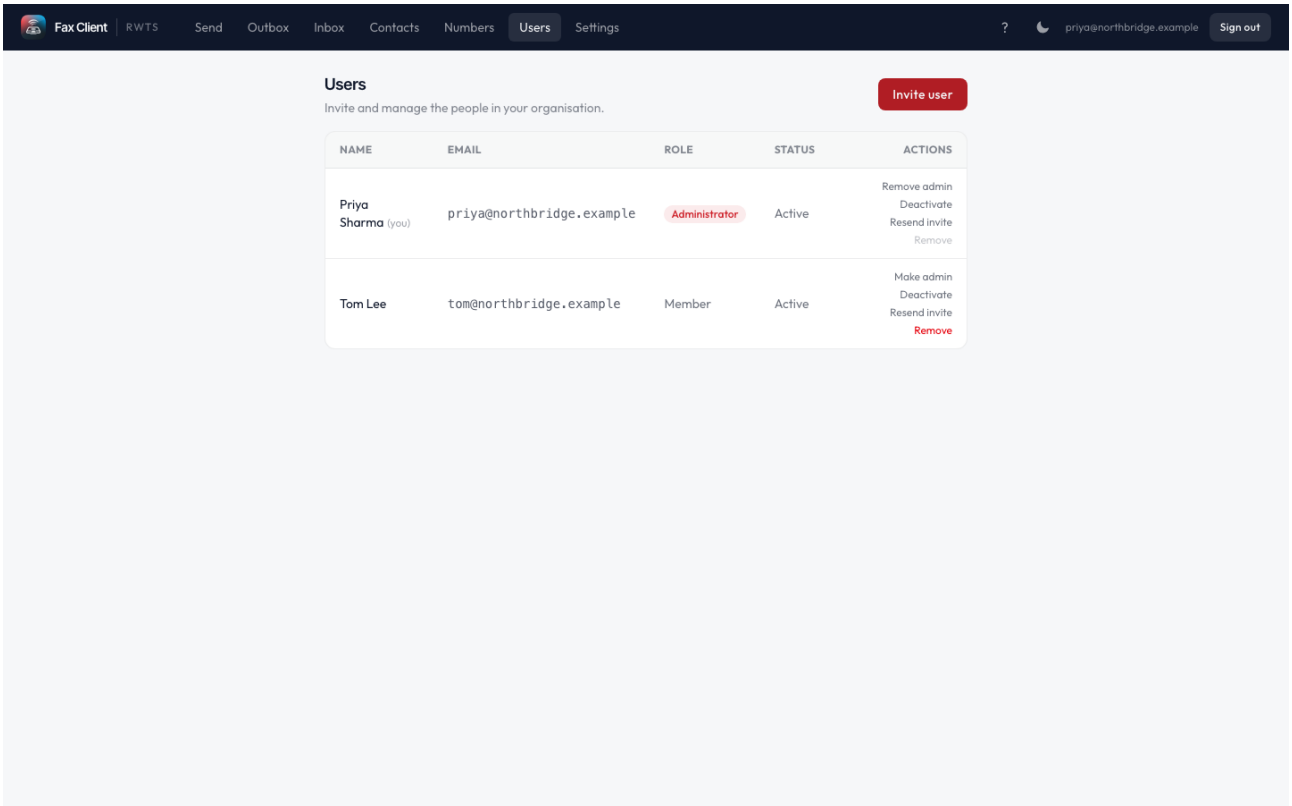


Figure 14: The Users page listing organisation members with their name, email, role and status

## What you can see

The Users page lists each person in your organisation with their:

- **Name** and **email address**
- **Role** — Administrator or Member
- **Status** — Active or Inactive

## Inviting someone

1. Click **Invite user**.
2. Enter their **email address**. Optionally add their **first name** and **last name**.
3. If they should be an administrator, tick the option to make them an administrator.

The person receives an email with a link to set their own password — you never set it for them.

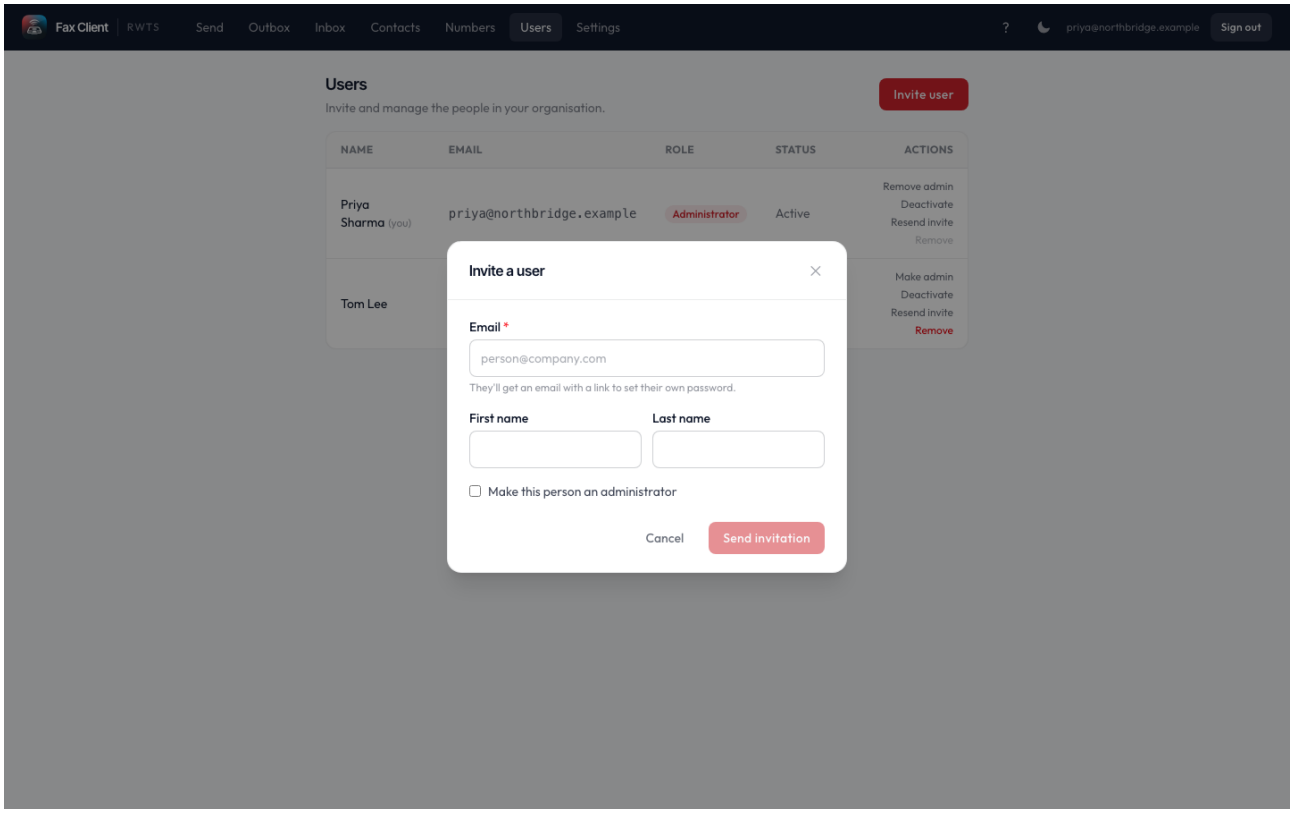


Figure 15: The Invite user form with fields for email, name and an administrator option

## Per-user actions

For each user in the list you can:

- **Make admin** / **Remove admin** — change their role between Administrator and Member.
- **Deactivate** / **Reactivate** — an inactive user cannot sign in.
- **Resend invite** — sends the set-password email again.
- **Remove** — takes them out of your organisation and disables their sign-in.

## What administrators can do

Administrators can do everything a member can, plus:

- Manage users.
- Manage sending identities.
- Manage fax-number delivery.

## Safeguards

Your organisation must always have at least one active administrator. Because of this:

- You cannot remove, deactivate, or demote the last active administrator.
- You cannot remove yourself.

# Sending identities (fax lines)

A sending identity is the fax line a message is sent from. You manage these on the **Settings** page.

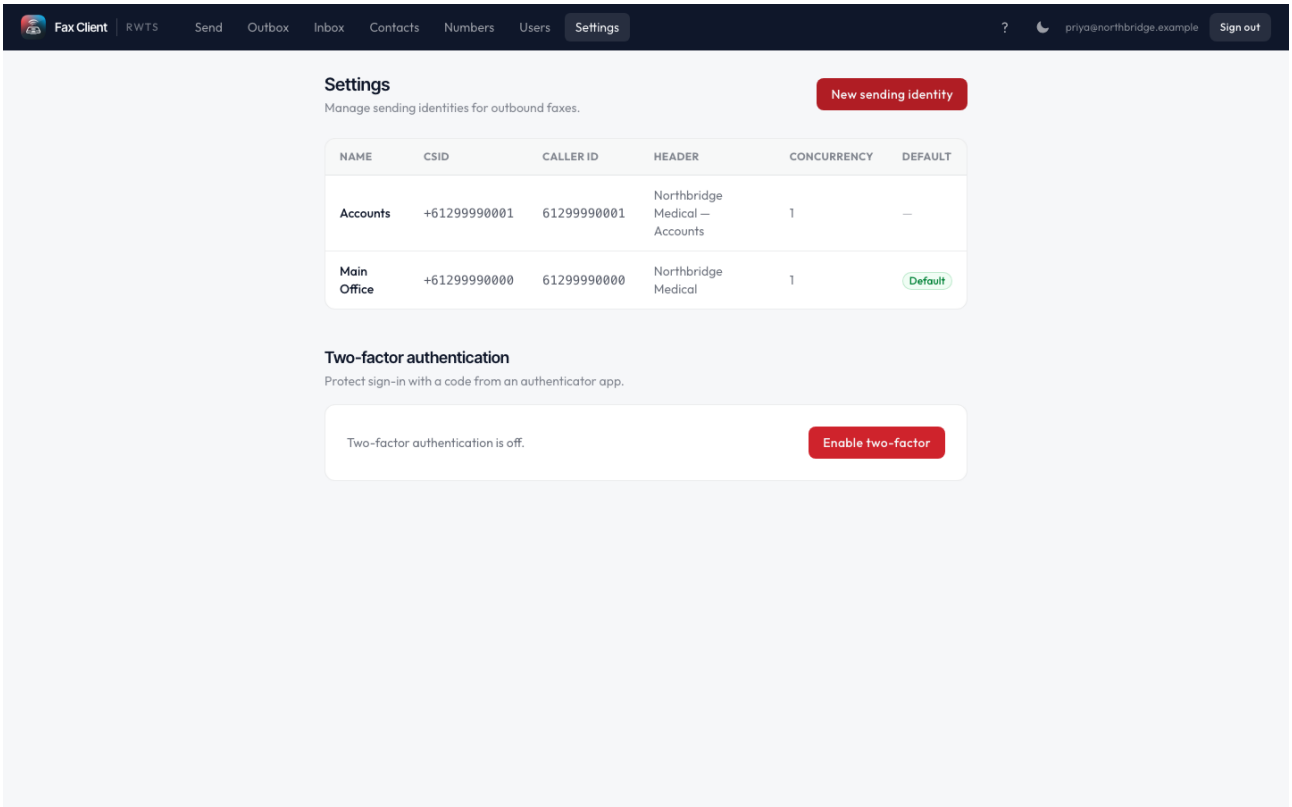


Figure 16: The Settings page listing your sending identities

The list shows each identity's **Name**, **CSID**, **Caller ID**, **Header**, and whether it is the default.

## Add a sending identity

1. Go to **Settings**.
2. Click **New sending identity**.
3. Fill in the fields:
   - **Name** — a label for the line, for example "Main Office".
   - **CSID** — the sender ID shown on the receiving fax machine, in international format.
   - **Caller ID** — the number transmitted as caller ID, in international format with no leading 0.
   - **Fax header** — the banner printed across the top of each page. Defaults to the identity name.
4. Save the identity.

## A few things to know

- One identity is the default and is pre-selected on the **Send** page.

- Only administrators can add or change sending identities.
- Members see identities as read-only and pick one when sending.

# Choosing who receives your faxes

The **Numbers** page lists your organisation's fax numbers. For each number, you control which email addresses receive a copy of every inbound fax.

## Set delivery addresses for a number

1. Open the **Numbers** page.
2. Find the fax number you want to configure.
3. In the **Delivery emails** field, enter one or more email addresses. Separate multiple addresses with commas.
4. Optionally, set a **Station** label to help identify the number.
5. Click **Save** to apply your changes.

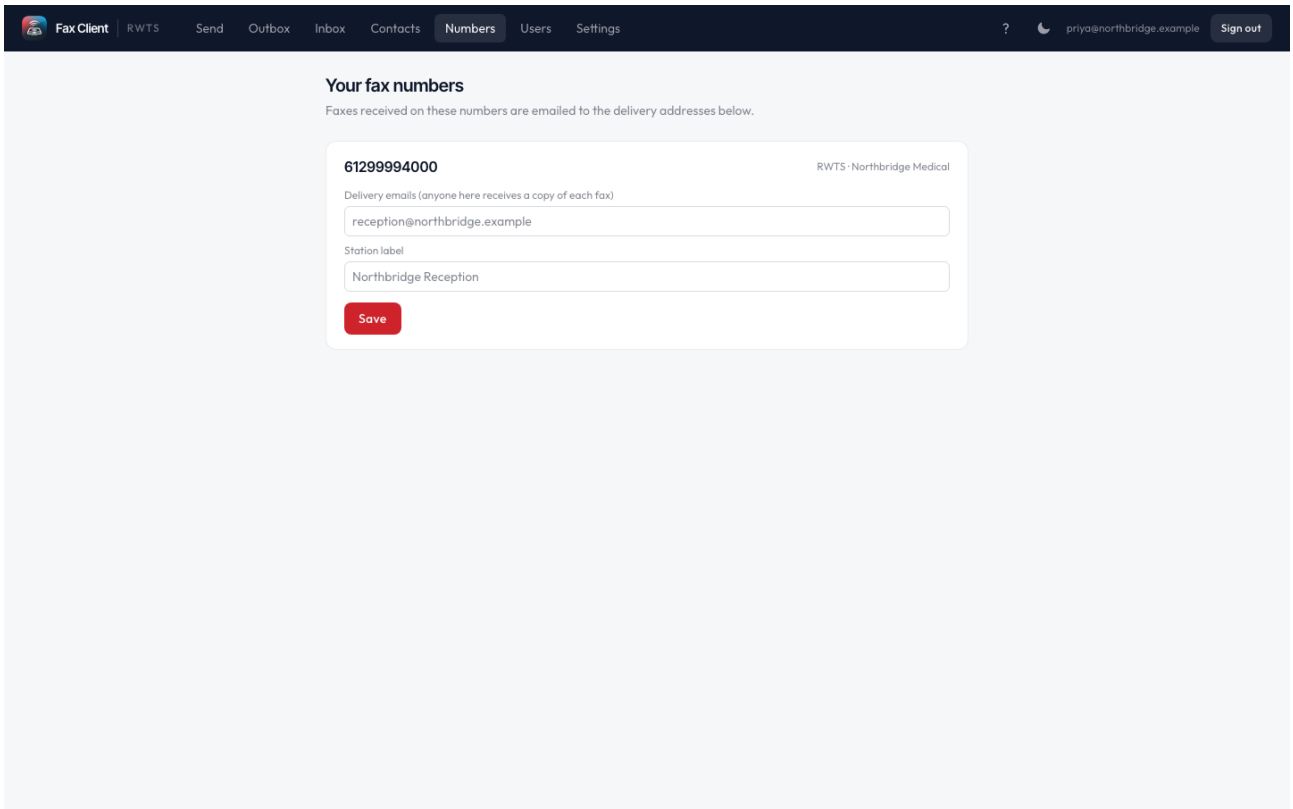


Figure 17: The Numbers page, where you set the delivery emails and station label for each fax number

## How delivery works

- Every address listed in **Delivery emails** receives its own private copy of each fax. Recipients cannot see who else is on the list.
- You can update the delivery addresses at any time by editing the field and clicking **Save**.

## What RWTS manages

- Provisioning new fax numbers, and enabling or disabling a number, is handled by RWTS or your provider.
- The “from” address is also managed by RWTS or your provider.
- You control who receives the faxes for your numbers.

# Requiring two-factor authentication

Your organisation can be set to require two-factor authentication (2FA) for everyone. When the requirement is on, each user is prompted to set up 2FA before they can use the app.

## How organisation-wide 2FA works

- When the requirement is on, each user is prompted to set up 2FA and cannot use the app until they complete setup.
- Turning the requirement on for your organisation is arranged through RWTS or your provider, as it is part of your organisation's security settings.
- Each user sets up their own 2FA from **Settings**. See the Two-factor authentication topic for the steps they need to follow.

## What you should do as an administrator

1. Contact RWTS or your provider to have the 2FA requirement turned on for your organisation.
2. Encourage your users to enrol promptly, directing them to **Settings** to set up their 2FA.
3. Follow up with anyone who has not yet enrolled, so they are not locked out of tasks.

real world technology solutions

# Setting up single sign-on

Single sign-on (SSO) lets your users sign in with the same identity your organisation already uses for everything else — Microsoft Entra ID, Google Workspace, Okta, Keycloak, or any other SAML 2.0 identity provider (IdP). Once it's set up, users on a verified email domain are sent straight to your IdP instead of typing a Fax Client password.

You manage all of this yourself from **Settings > Single Sign-On** — there's nothing for RWTS to configure on your behalf.

## What you'll do, in order

1. Verify the email domain(s) your users sign in with.
2. Register Fax Client as an application in your identity provider, using the SP details from the settings page.
3. Enter your identity provider's details into Fax Client.
4. Map your IdP's attributes to Fax Client roles.
5. Optionally, require SSO for everyone in your organisation.

## Step 1: Verify your email domain

SSO only ever applies to email domains you've proven you own. Under **Verified domains**:

1. Add the domain your users sign in with, for example `acme.example`.
2. Fax Client generates a one-time verification token for that domain.
3. Create a DNS TXT record at `_faxgateway-verify.<your-domain>` with the value `faxgateway-verify=<token>` shown on the page.
4. Click **Verify now**. Fax Client looks up the TXT record and marks the domain verified once it finds a match.

A domain that isn't verified is never used for sign-in — adding it is not enough on its own. You can add more than one domain if your organisation sends mail from several.

## Step 2: Register Fax Client with your identity provider

Every IdP needs three things from Fax Client, all shown on the **Settings > Single Sign-On** page under **Your SP details**:

- **SP entity ID / metadata URL** — the identifier for this application, and the URL your IdP can fetch full SAML metadata from.
- **ACS URL** — the Assertion Consumer Service URL, where your IdP sends the user back after they sign in.

Copy these into your IdP when you create the application/enterprise app entry. The exact field names differ by provider — see the guide for your IdP for the specifics:

- Microsoft Entra ID
- Google Workspace
- Keycloak
- Okta (and Duo SSO)

Fax Client identifies users by email address (NameID), so make sure your IdP is configured to send the user's email as the SAML NameID.

Fax Client also requires the IdP to sign the SAML **assertion** specifically (not just the outer response envelope). Microsoft Entra ID, Okta, and Google Workspace all do this by default, so there's usually nothing to change. Keycloak has its own explicit toggle for it — see the per-provider guide for exactly where. If sign-in ever fails with "Invalid SAML assertion", this is the first thing to check.

### Step 3: Enter your IdP's details

Back in Fax Client, fill in:

- **IdP entity ID** — your identity provider's entity ID.
- **IdP SSO URL** — where Fax Client sends users to sign in.
- **IdP signing certificate** — the X.509 certificate your IdP uses to sign its responses, so Fax Client can verify them.

Fax Client doesn't sign its own requests — there's no SP signing key to generate or exchange. You only ever need to give your IdP the SP entity ID and ACS URL from Step 2.

### Step 4: Map attributes to roles

Role mappings decide what a user becomes in Fax Client based on an attribute your IdP sends in the SAML assertion — for example, mapping a `role` attribute value of `admin` to **Tenant admin**, and everything else to **Member**.

- Add one mapping per attribute value you care about.
- Set a **default role** for users who don't match any mapping, or leave it blank and turn on **Reject sign-in for unmapped users** so anyone without a matching attribute is refused rather than silently given a default role.
- The first time a user signs in via SSO who doesn't already have a Fax Client account, one is created automatically (just-in-time provisioning) with the mapped role.
- A user who already has an account in a *different* organisation can never be pulled into yours by SSO — sign-in for that account is rejected outright, and nothing is changed on their existing account.

### Step 5: Require SSO (optional)

Turning on **Require SSO (disable password login for this organisation)** stops everyone else in your organisation from signing in with a password — they must use SSO from then on.

Turning on enforcement never locks out your own emergency access. **Superusers** can always sign in with a password, and you can nominate one of your own users as the **emergency admin** for your organisation — that person can also still use a password if your identity provider is ever unreachable. Set an emergency admin *before* you turn enforcement on.

### A few things to know

- SSO is SAML 2.0 only. There's no OAuth/OIDC option.
- Enforcement only takes effect while your SSO configuration is actually active — if it's turned off, or your plan no longer includes SSO, password login keeps working for everyone as a safety net.
- Whether SSO is available at all on your plan is arranged through RWTS or your provider, the same as any other plan change.

real world technology solutions

# SSO setup: Microsoft Entra ID

This guide walks through registering Fax Client as a SAML enterprise application in Microsoft Entra ID (formerly Azure AD). Before you start, open **Settings > Single Sign-On** in Fax Client in another tab — you'll need the **SP entity ID / metadata URL** and **ACS URL** shown there.

## 1. Create the enterprise application

1. Sign in to the Microsoft Entra admin center as a Global Administrator or Application Administrator.
2. Go to **Identity > Applications > Enterprise applications > New application**.
3. Choose **Create your own application**, give it a name (for example "Fax Client"), and select **Integrate any other application you don't find in the gallery (Non-gallery)**.

## 2. Configure single sign-on

1. Open the new application, then **Single sign-on > SAML**.
2. Under **Basic SAML Configuration**, set:
   - **Identifier (Entity ID)** — paste the **SP entity ID / metadata URL** from Fax Client's settings page.
   - **Reply URL (Assertion Consumer Service URL)** — paste the **ACS URL** from Fax Client's settings page.
3. Under **Attributes & Claims**, set the **Unique User Identifier (Name ID)** claim's source to the user's email address, with the NameID format set to **Email address**. Fax Client matches users by email, so this step is required.
4. Add a claim for the role Fax Client should map — for example a claim named `role` sourced from a user attribute or group membership, carrying a value such as `admin` or `member`. You'll match on this claim's name and value in Fax Client's role mappings.
5. Leave **Signing Option** under **SAML Certificates** at its default, **Sign SAML assertion**. Entra ID signs the assertion by default, and Fax Client specifically requires the assertion to be signed — not just the outer response envelope — so there's nothing to change here unless a previous configuration turned assertion signing off.

## 3. Give Fax Client the IdP details

Still on the **Single sign-on** page, scroll to **SAML Certificates** and **Set up Fax Client**, and copy the following back into Fax Client's **Settings > Single Sign-On**:

- **Login URL** → Fax Client's **IdP SSO URL**.
- **Microsoft Entra Identifier** → Fax Client's **IdP entity ID**.
- The **Certificate (Base64)** from SAML Certificates → Fax Client's **IdP signing certificate** (paste the whole PEM block, including the `BEGIN CERTIFICATE` / `END CERTIFICATE` lines).

### 4. Assign users

Under **Users and groups**, assign the users or groups who should have access. Entra only sends assertions for assigned users — anyone not assigned is refused sign-in by Entra before Fax Client is even involved.

### 5. Finish in Fax Client

Back in Fax Client, add a role mapping for the claim you configured in step 2 (attribute name `role`, the value you chose, and the Fax Client role it should grant), then verify your email domain if you haven't already. A test sign-in from the Entra **My Apps** portal, or from the Fax Client login page with an email on your verified domain, should redirect straight to Entra and back.

real world technology solutions

# SSO setup: Google Workspace

This guide walks through registering Fax Client as a custom SAML application in Google Workspace. Before you start, open **Settings > Single Sign-On** in Fax Client in another tab — you'll need the **SP entity ID / metadata URL** and **ACS URL** shown there.

## 1. Add a custom SAML app

1. Sign in to the Google Admin console as a super admin.
2. Go to **Apps > Web and mobile apps > Add app > Add custom SAML app**.
3. Name it (for example "Fax Client") and continue past the icon step if you don't have a logo to upload.

## 2. Copy Google's IdP details into Fax Client

On the **Google Identity Provider details** screen, Google shows you its SSO URL, Entity ID, and a downloadable certificate. Copy these into Fax Client's **Settings > Single Sign-On**:

- **SSO URL** → Fax Client's **IdP SSO URL**.
- **Entity ID** → Fax Client's **IdP entity ID**.
- **Certificate** (download it, open it in a text editor) → Fax Client's **IdP signing certificate**, pasted in full including the `BEGIN CERTIFICATE` / `END CERTIFICATE` lines.

Click **Continue**.

## 3. Give Google Fax Client's service provider details

On the **Service provider details** screen:

- **ACS URL** — paste the **ACS URL** from Fax Client's settings page.
- **Entity ID** — paste the **SP entity ID / metadata URL** from Fax Client's settings page.
- **Name ID format** — select **EMAIL**.
- **Name ID** — select **Basic information > Primary email**. Fax Client matches users by email, so this must be their email address.

Click **Continue**.

## 4. Map attributes

On the **Attribute mapping** screen, add a mapping that sends the role information Fax Client needs — for example, map a Google user attribute or organisational unit to an attribute named `role`, carrying a value such as `admin` or `member`. You'll match on this attribute's name and value in Fax Client's role mappings. Click **Finish**.

### 5. Confirm the assertion is signed

Fax Client validates the signature on the SAML **assertion**, not the outer response envelope. Google Workspace signs the assertion by default for custom SAML apps, but if this app's signing behaviour has ever been changed, go back into the app and check under **Service provider details** (or the app's settings) that assertion signing is still turned on before continuing — a response-only signature will make sign-in fail with an "Invalid SAML assertion" error.

### 6. Turn the app on for your users

Custom SAML apps are **off** for everyone by default. Open the new app, go to **User access**, and turn it **ON** for the organisational units or groups who should have access.

### 7. Finish in Fax Client

Back in Fax Client, add a role mapping for the attribute you configured in step 4, then verify your email domain if you haven't already. A test sign-in from Google's app launcher, or from the Fax Client login page with an email on your verified domain, should redirect straight to Google and back.

real world technology solutions

# SSO setup: Keycloak

This guide walks through registering Fax Client as a SAML client in Keycloak. Before you start, open **Settings > Single Sign-On** in Fax Client in another tab — you'll need the **SP entity ID / metadata URL** and **ACS URL** shown there.

## 1. Create the SAML client

1. Sign in to the Keycloak admin console and select the realm your users belong to.
2. Go to **Clients > Create client**.
3. Set **Client type** to **SAML**.
4. Set **Client ID** to the **SP entity ID / metadata URL** from Fax Client's settings page — this is the SP's entity ID, and Keycloak uses the Client ID field for it.

## 2. Configure the client's SAML settings

On the client's **Settings** tab:

- **Home URL** — optional; you can leave this blank or set it to your Fax Client login page.
- **Valid redirect URIs** — add the **ACS URL** from Fax Client's settings page. This is where Keycloak sends the user back after signing in.
- **Master SAML Processing URL** — set this to the same ACS URL; Keycloak uses it as the default Assertion Consumer Service URL if a per-binding one isn't set.
- **Name ID format** — set to **email**. Fax Client matches users by email, so this is required.
- **Sign documents** and **Sign assertions** — turn these **on**. **Sign assertions** is the one that matters most: Fax Client validates the signature on the SAML assertion itself, not just the outer response, so this must be on even if you leave **Sign documents** off. Fax Client verifies the IdP's signature using the certificate you'll copy in step 4.

## 3. Add a role/attribute mapper

Go to the client's **Client scopes** tab, open the dedicated scope for this client, and **Add mapper**. Add a mapper that sends a role or group value as a SAML attribute — for example an attribute named `role` populated from the user's Keycloak realm role or group membership, carrying a value such as `admin` or `member`. You'll match on this attribute's name and value in Fax Client's role mappings.

## 4. Copy Keycloak's IdP details into Fax Client

Under **Realm settings > General > Endpoints**, open the **SAML 2.0 Identity Provider Metadata** link (or download it). From the metadata, copy into Fax Client's **Settings > Single Sign-On**:

- The realm's `entityID` → Fax Client's **IdP entity ID**.
- The SSO redirect binding `Location` → Fax Client's **IdP SSO URL**.

- The `X509Certificate` value → Fax Client's **IdP signing certificate** (Fax Client accepts the raw base64, with or without the `BEGIN CERTIFICATE` / `END CERTIFICATE` wrapper).

### 5. Assign users

Grant the client role, realm role, or group you mapped in step 3 to the users who should have access.

### 6. Finish in Fax Client

Back in Fax Client, add a role mapping for the attribute you configured in step 3, then verify your email domain if you haven't already. A test sign-in from Keycloak's account console, or from the Fax Client login page with an email on your verified domain, should redirect straight to Keycloak and back.

real world technology solutions

# SSO setup: Okta (and Duo SSO)

This guide walks through registering Fax Client as a SAML app in Okta. If your organisation uses Duo SSO instead — Duo's hosted SAML identity provider, often sitting in front of Okta or another directory — the same fields apply; a short note on that is at the end.

Before you start, open **Settings > Single Sign-On** in Fax Client in another tab — you'll need the **SP entity ID / metadata URL** and **ACS URL** shown there.

## 1. Create the app integration

1. Sign in to the Okta admin console.
2. Go to **Applications > Applications > Create App Integration**.
3. Choose **SAML 2.0** and give the app a name (for example "Fax Client").

## 2. Configure SAML settings

On the **Configure SAML** step:

- **Single sign-on URL** — paste the **ACS URL** from Fax Client's settings page.
- **Audience URI (SP Entity ID)** — paste the **SP entity ID / metadata URL** from Fax Client's settings page.
- **Name ID format** — select **EmailAddress**.
- **Application username** — select **Email**. Fax Client matches users by email, so this must resolve to their email address.

Under **Attribute Statements**, add a statement that sends the role information Fax Client needs — for example an attribute named `role` sourced from an Okta profile attribute or group, carrying a value such as `admin` or `member`. You'll match on this attribute's name and value in Fax Client's role mappings.

Leave **Response** and **Assertion Signature** under the **Advanced Settings** section at their Okta defaults — Okta signs the assertion by default, which is exactly what Fax Client requires (it validates the assertion's signature, not the outer response envelope). There's nothing to change here unless assertion signing has previously been turned off for this app.

## 3. Copy Okta's IdP details into Fax Client

After finishing setup, open the app's **Sign On** tab and click **View SAML setup instructions**. Copy the following into Fax Client's **Settings > Single Sign-On**:

- **Identity Provider Single Sign-On URL** → Fax Client's **IdP SSO URL**.
- **Identity Provider Issuer** → Fax Client's **IdP entity ID**.
- **X.509 Certificate** → Fax Client's **IdP signing certificate**, pasted in full including the `BEGIN CERTIFICATE` / `END CERTIFICATE` lines.

### 4. Assign users

On the app's **Assignments** tab, assign the people or groups who should have access. Okta only sends assertions for assigned users.

### 5. Finish in Fax Client

Back in Fax Client, add a role mapping for the attribute statement you configured in step 2, then verify your email domain if you haven't already. A test sign-in from the Okta end-user dashboard, or from the Fax Client login page with an email on your verified domain, should redirect straight to Okta and back.

### Using Duo SSO instead

If your organisation uses Duo SSO as the identity provider (rather than Okta directly), the setup is the same shape: in the Duo Admin Panel, add a **Generic SAML Service Provider** application, supply the same **ACS URL** as the Assertion Consumer Service and the same **SP entity ID / metadata URL** as the Entity ID/Audience, set the NameID to the user's email, and add an attribute for the role claim. Copy Duo's **Single Sign-On URL**, **Entity ID**, and certificate into Fax Client exactly as described above for Okta. Duo signs the assertion by default too, so no extra step is needed — just confirm assertion signing hasn't been disabled if this application was cloned from an existing one.