real world technology solutions

ADMINISTRATOR GUIDE

SMS Client

Managing team logins, administrator access, number permissions, and message oversight.

AUTHOR
Real World Technology Solutions

DATE
August 2026

real world technology solutions

Contents

Administration Area Overview

As an administrator, you have access to a dedicated administration area where you can manage logins for your team, control who has administrator access, decide which numbers each person can use, and review your organisation's message history.

What you can do here

The administration area is divided into four sections in the left-hand navigation:

- **Accounts** — manage team logins (**Users**) and administrator access (**Memberships**).
- **Contacts** — view and manage your organisation's contacts and tags.
- **Messaging** — browse your organisation's **Conversations** and read the full **Messages** history.
- **Senders** — control which numbers each person can use via **Sender assignments**, and view available numbers under **Sender resources**.

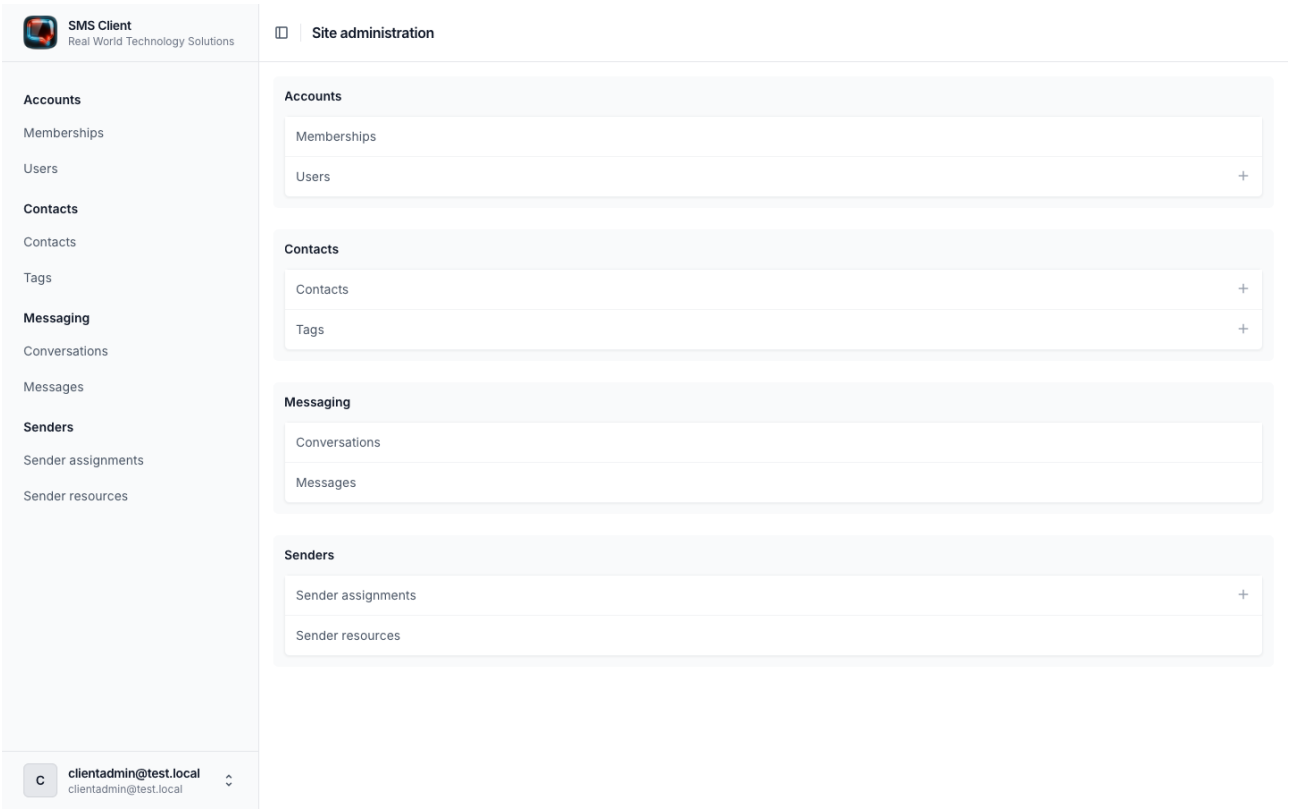

Figure 1: The administration area dashboard showing sections for Accounts, Contacts, Messaging, and Senders

How to get to the administration area

Go to `https://smsclient.rwts.com.au/admin`. Sign in with your administrator email and password. See Signing in to the administration area for step-by-step instructions.

What you won't see here

You only see data for your own organisation. Settings for the platform itself, other organisations, or technical infrastructure are managed separately and are not visible in your administration area.

Signing In to the Administration Area

The administration area is a separate login from the main SMS Client app — you sign in at `https://smsclient.rwts.com.au/admin` using your administrator email address and password.

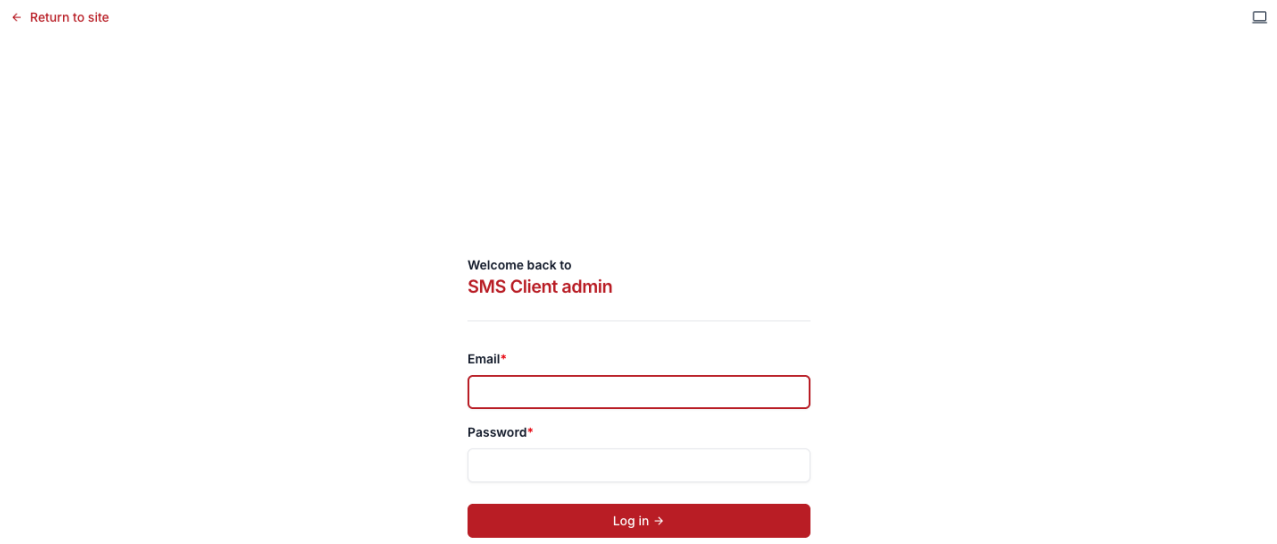

Figure 2: The SMS Client admin sign-in screen showing Email and Password fields and a Log in button

1. In your browser, go to `https://smsclient.rwts.com.au/admin`.
2. Enter your administrator email address in the **Email** field.
3. Enter your password in the **Password** field.
4. Click **Log in**.

You will land on the administration area dashboard showing all available sections.

If sign-in doesn't work

- Double-check your email address for typos.
- Make sure Caps Lock is off when typing your password.
- Confirm you are using `https://smsclient.rwts.com.au/admin`, not the main app address — they require separate logins.
- If you still cannot get in, contact your platform provider to have your administrator account checked or your password reset.

Adding a Login for a Team Member

When someone new joins your team, you create a login for them in the administration area. The account is automatically connected to your organisation — there is nothing extra to link up.

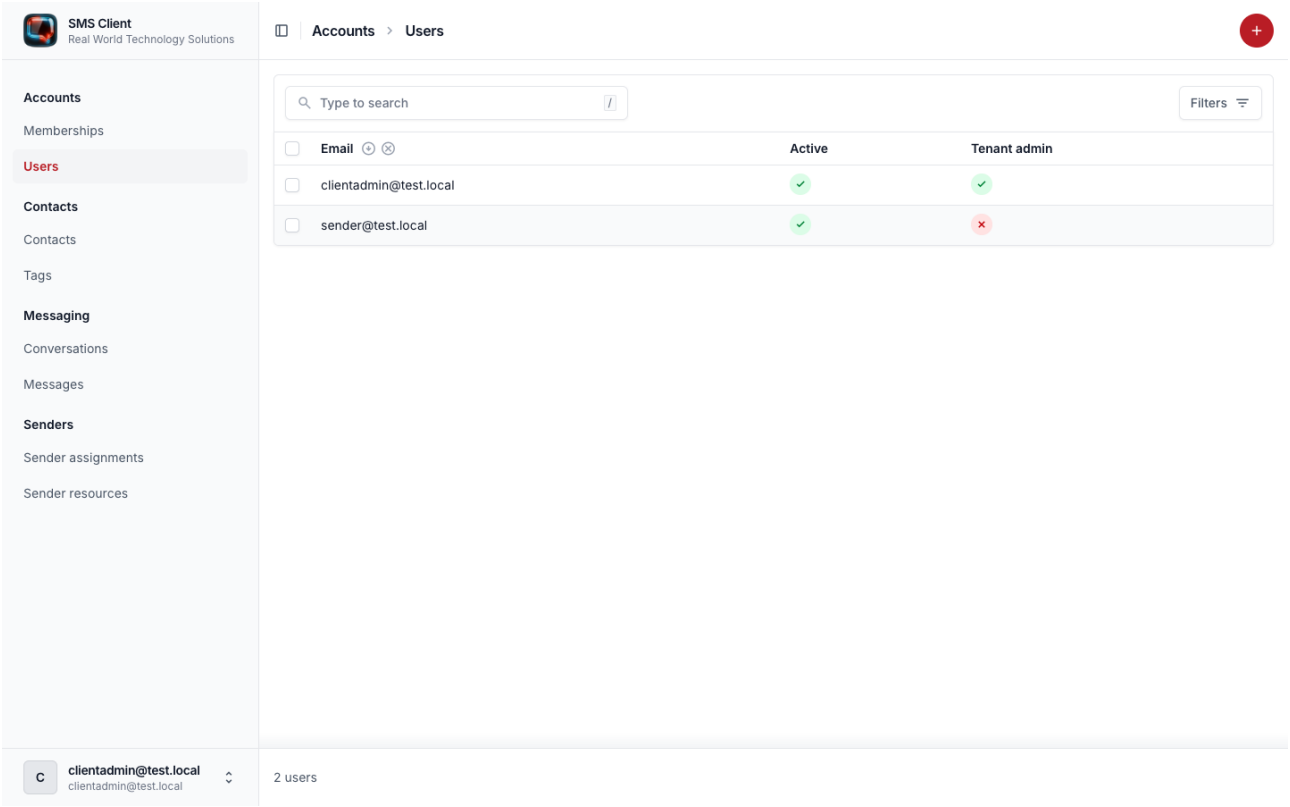

Figure 3: The Users list showing two accounts with Active and Tenant admin columns

1. In the left-hand navigation, click **Users** under **Accounts**.
2. Click the **+** button in the top-right corner of the page.
3. Enter the person's email address in the **Email** field.
4. Enter a password in the **Password** field, then enter it again in the **Password confirmation** field.
5. Click **Save**.

The new login appears in the **Users** list. That person can now sign in to the SMS Client app using the email address and password you set.

Next steps

- To let the person send or receive messages on a specific number, see Controlling number permissions.
- To give the person administrator access to the administration area, see Making someone an administrator.

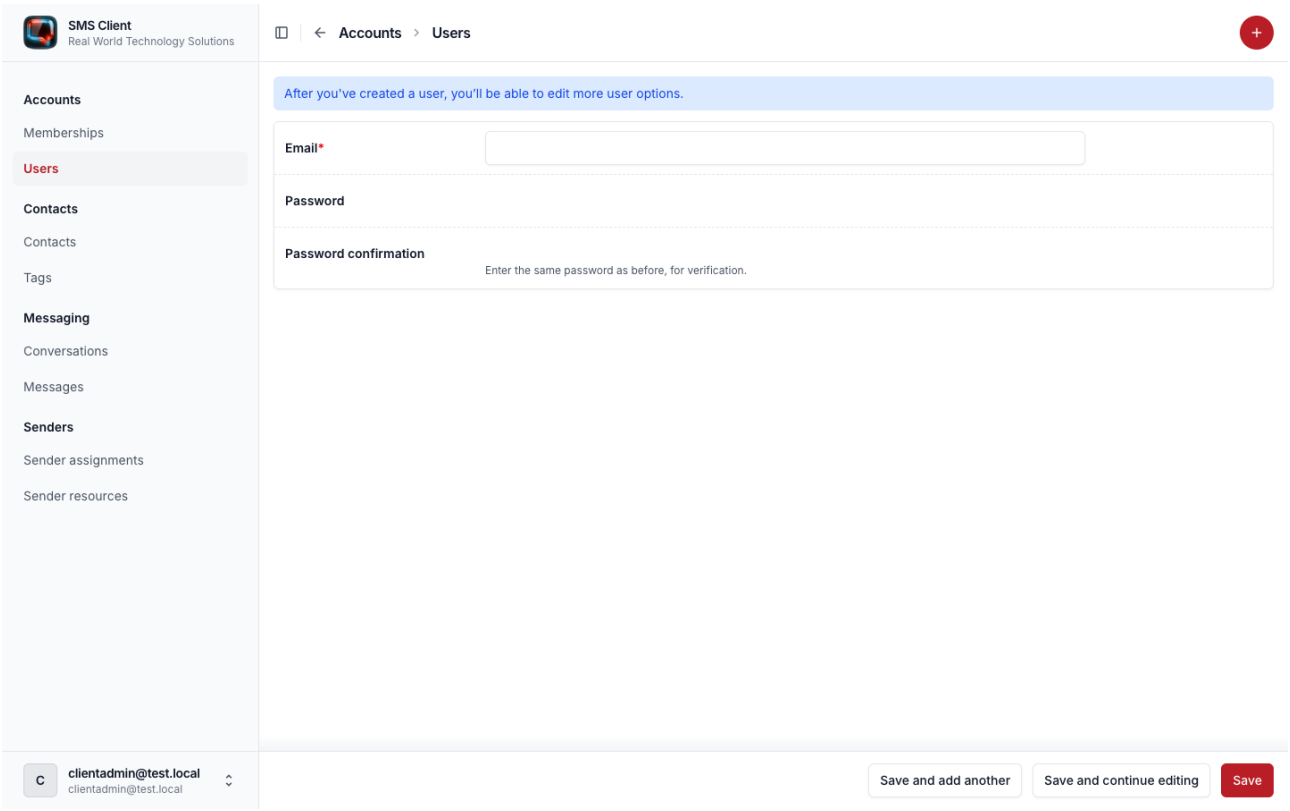

Figure 4: The Add user form with Email, Password, and Password confirmation fields

Changing a password later

Open the user from the **Users** list and use the password fields to set a new one, then click **Save**.

Making Someone an Administrator

Each person in your organisation has a membership record that links their login to your organisation. Turning on the **Is tenant admin** toggle promotes them to administrator — they will gain access to the administration area and can manage the team just as you can. Turning it off removes that access.

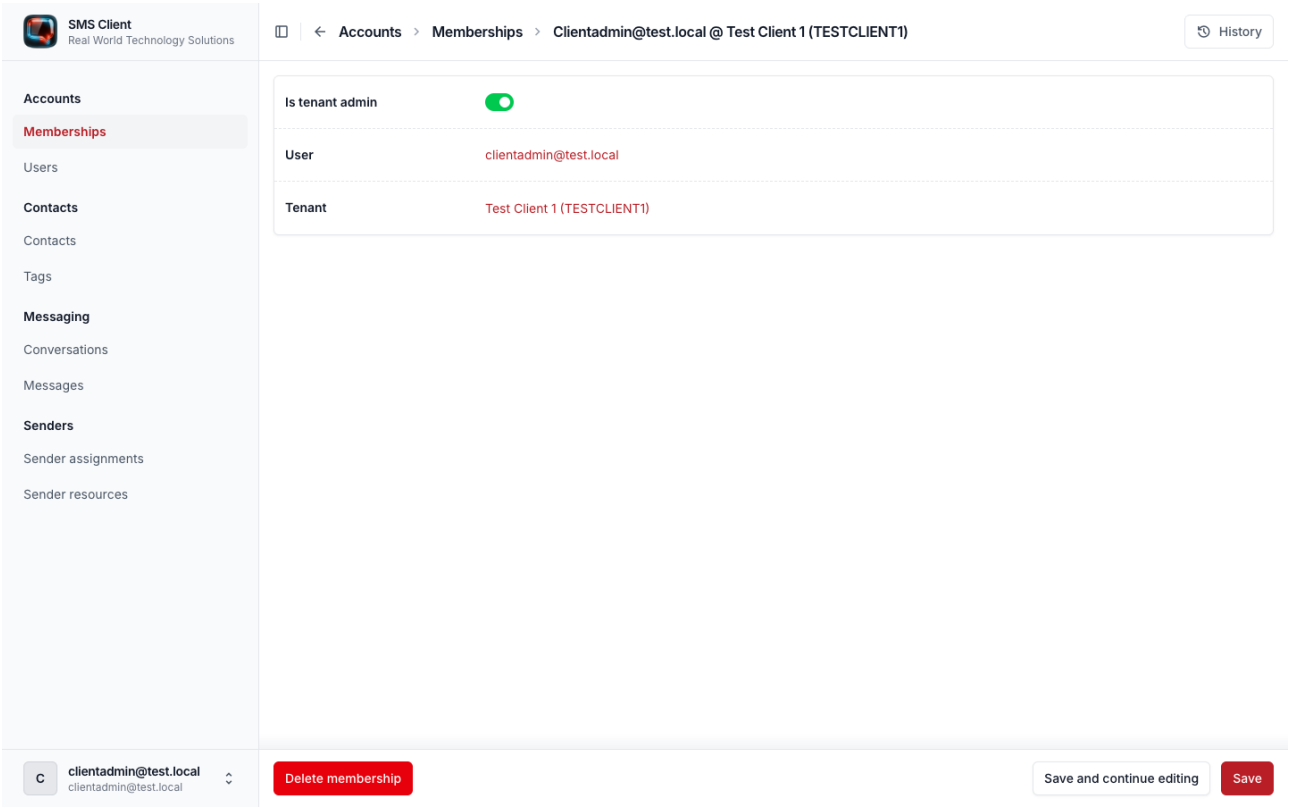

Figure 5: The membership detail page for a user showing the Is tenant admin toggle switched on, along with the User and Tenant fields

Granting administrator access

1. In the left-hand navigation, click **Memberships** under **Accounts**.
2. Click the name of the person you want to promote.
3. Switch the **Is tenant admin** toggle on (it turns green).
4. Click **Save**.

That person can now sign in to the administration area at `/admin` and manage users and settings for your organisation.

Removing administrator access

1. In the left-hand navigation, click **Memberships** under **Accounts**.
2. Click the name of the person whose access you want to remove.

3. Switch the **Is tenant admin** toggle off (it turns grey).
4. Click **Save**.

Their login to the main SMS Client app is not affected — they can still use the app, they just no longer have access to the administration area.

Things to keep in mind

- You will always see your own membership in the list. Be careful not to accidentally remove your own administrator access.
- At least one person in your organisation should have administrator access at all times.

Controlling Number Permissions

A sender assignment connects a team member to a specific phone number and controls exactly what they can do with it. You can grant or restrict sending and receiving independently for each person and number combination.

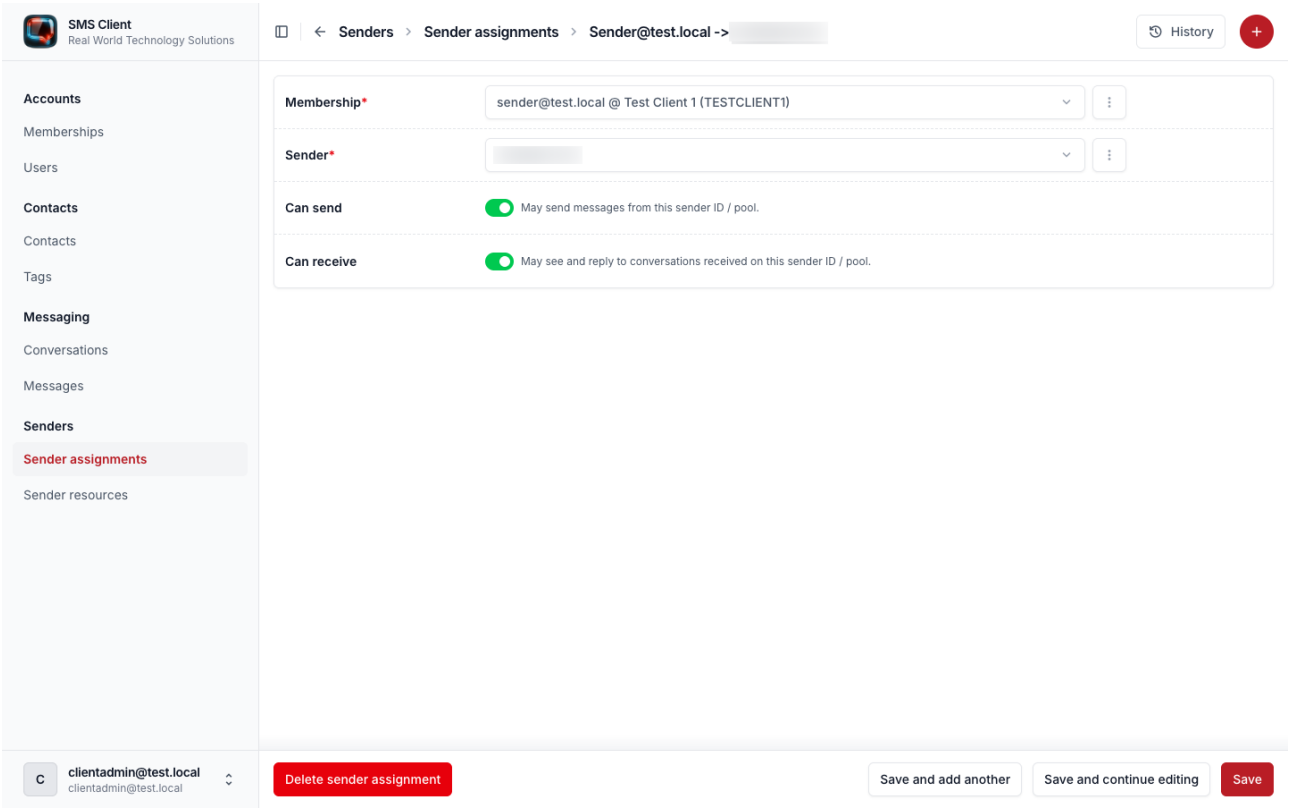

Figure 6: The sender assignment detail page showing Membership, Sender, Can send, and Can receive fields

What the two permissions mean

- **Can send** — the person may send messages from that number in the SMS Client app.
- **Can receive** — the person may see conversations that arrive on that number.

These two settings are independent. For example, you can let someone read incoming messages on a shared number without allowing them to send from it, or allow sending only.

Adding a new sender assignment

1. In the left-hand navigation, click **Sender assignments** under **Senders**.
2. Click the **+** button in the top-right corner of the page.
3. Choose the person from the **Membership** dropdown. Names are shown as the email address followed by your organisation name.

4. Choose the number from the **Sender** dropdown.
5. Switch **Can send** on or off depending on whether the person should be able to send from this number.
6. Switch **Can receive** on or off depending on whether the person should see conversations on this number.
7. Click **Save**.

Changing an existing sender assignment

1. In the left-hand navigation, click **Sender assignments** under **Senders**.
2. Click the assignment you want to change (shown as the email address and number).
3. Adjust the **Can send** and/or **Can receive** toggles as needed.
4. Click **Save**.

Removing a sender assignment

Open the assignment and click **Delete sender assignment** at the bottom of the page. The person will immediately lose access to that number in the app.

Viewing Message History

The **Messages** section gives you a read-only view of every message sent and received across your organisation — useful for oversight, resolving disputes, or checking on activity.

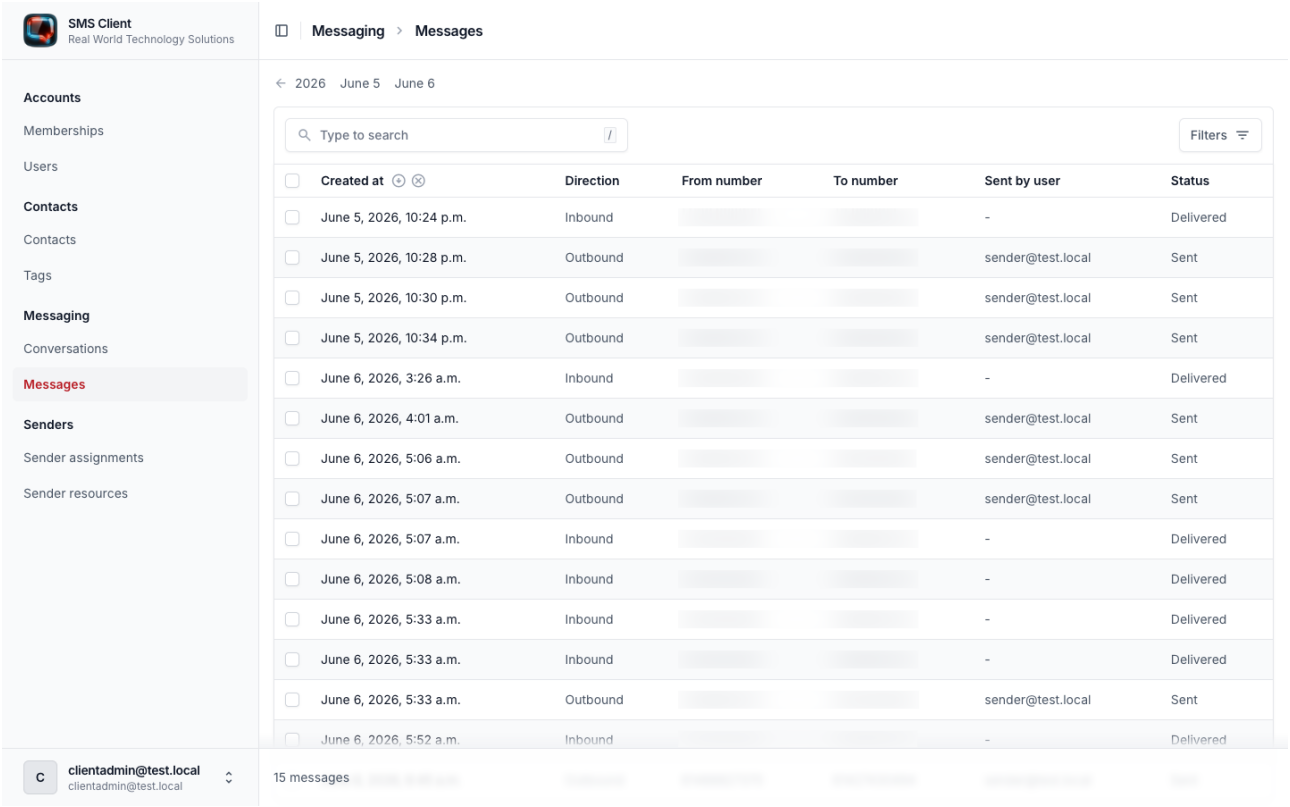

Figure 7: The Messages list showing columns for Created at, Direction, From number, To number, Sent by user, and Status, with date navigation at the top

Opening message history

1. In the left-hand navigation, click **Messages** under **Messaging**.

The list shows all messages for your organisation with the following columns:

- **Created at** — date and time the message was recorded.
- **Direction** — **Inbound** (a message arriving at one of your numbers) or **Outbound** (a message sent by a team member).
- **From number** — the number the message was sent from.
- **To number** — the number the message was sent to.
- **Sent by user** — for outbound messages, the team member who sent it. Inbound messages show a dash here.
- **Status** — for example, **Sent** or **Delivered**.

Filtering and searching

- Use the date navigation at the top of the list to step through messages by day.
- Click **Filters** in the top-right corner to narrow the list further (for example, by direction or number).
- Type in the **Type to search** box to search by content or number.

This view is read-only — you cannot send, edit, or delete messages from here.

Conversation Retention & Deletion Policy

You decide what happens when someone on your team deletes a conversation, and how long deleted conversations are kept before they are removed for good. These settings apply to your whole organisation.

> **Plan note:** changing the retention policy and viewing the audit trail are included from the **Team** plan. On Essentials, the defaults (soft delete, 90-day retention) are managed for you — see *Your Plan & Monthly Usage*.

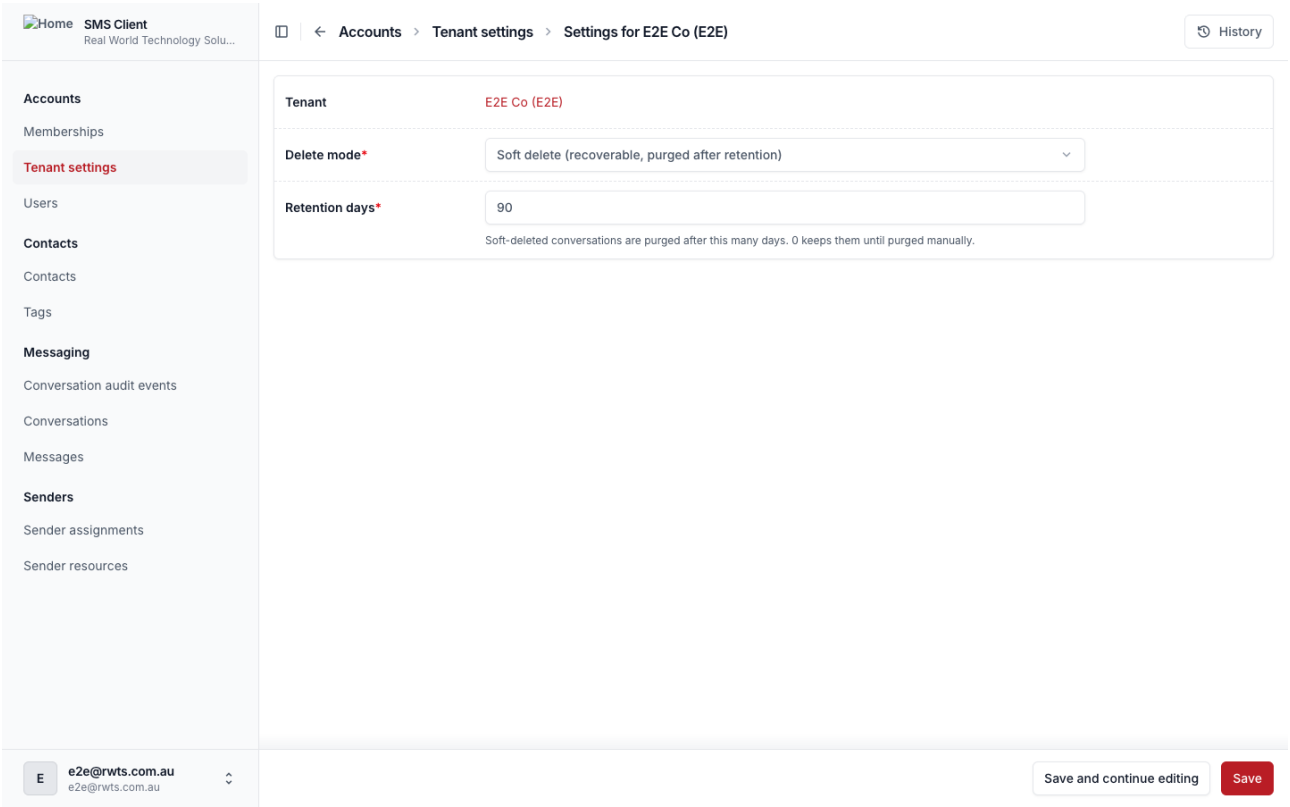

Figure 8: The Tenant settings form showing Delete mode and Retention days

Setting your policy

1. In the left-hand navigation, open **Tenant settings** (under **Accounts**).
2. Choose a **Delete mode**:
   - **Soft delete (recoverable)** — when a team member deletes a conversation, it is hidden from everyone but kept behind the scenes, so it can be restored and is automatically removed later (see **Retention days**). This is the safer default.
   - **Hard delete (permanent)** — deleting a conversation removes it and all of its messages immediately, with no way to recover it.

3. Set **Retention days** — for soft delete, how many days a deleted conversation is kept before it is permanently purged. For example, `90` keeps deleted conversations for about three months. Set it to `0` to keep them until you purge them yourself.
4. Click **Save**.

Restoring or permanently removing conversations

Open **Conversations** (under **Messaging**) to manage deleted conversations.

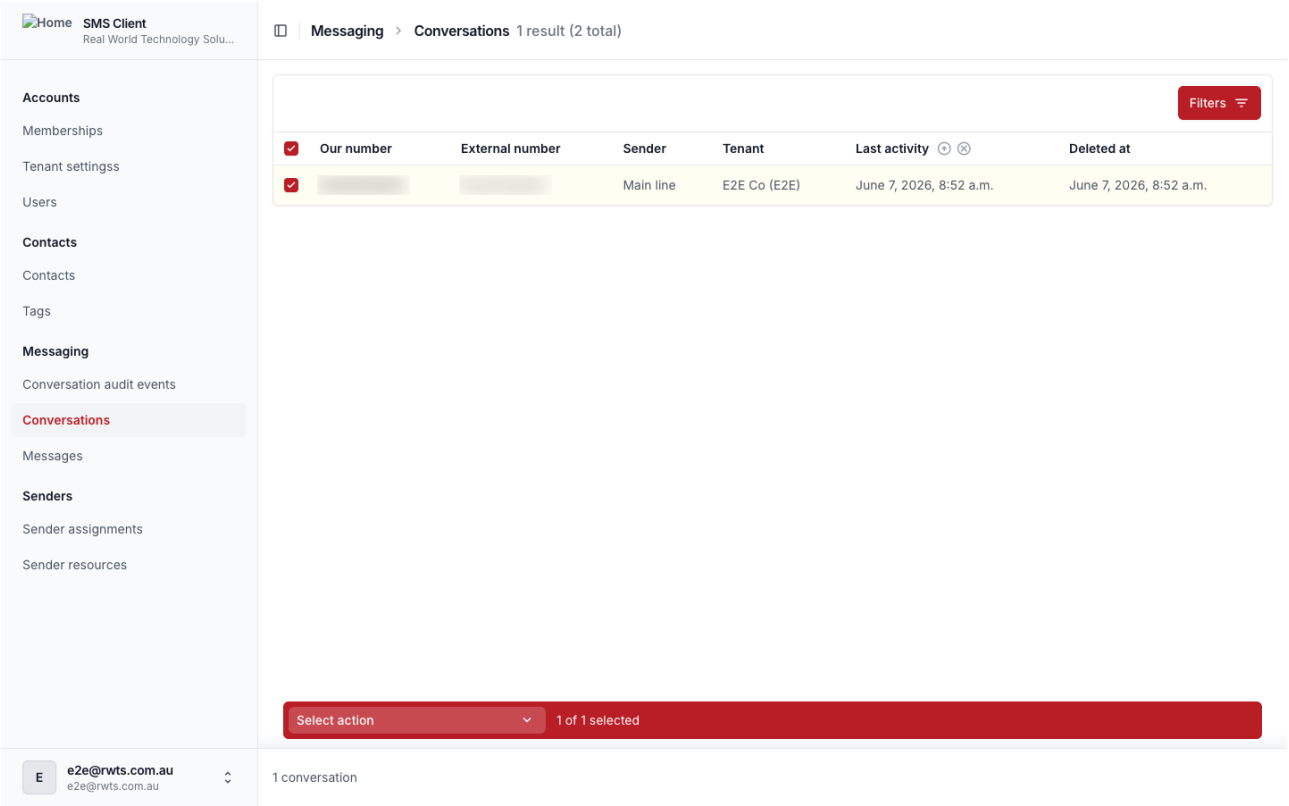

Figure 9: The Conversations list with the Deleted filter and the Restore / Purge actions

- Use the **Deleted** filter (top right) to show **Live**, **Deleted**, or all conversations.
- Tick one or more conversations, then choose an action:
  - **Restore selected conversations** — clears the deletion and makes them visible to your team again.
  - **Purge selected conversations (permanent)** — removes them and their messages for good. Use this with care; it cannot be undone.

Conversations are shown here for review only — you cannot edit a conversation's contents; you can restore or purge it.

The audit trail

Every delete, restore, purge, and export is recorded. Open **Conversation audit events** (under **Messaging**) to see who did what and when — useful for oversight and compliance. The log keeps the conversation reference and only the last few digits of the number, never the full number.

Session Timeouts & Two-Step Verification

The **Tenant settings** screen controls how long your team stays signed in and shows whether two-step verification is required for your organisation. (The same screen also holds your conversation retention policy — see *Conversation Retention & Deletion Policy*.)

> **Plan note:** custom session lifetimes and organisation-wide enforced 2FA are included from the **Team** plan — see *Your Plan & Monthly Usage*.

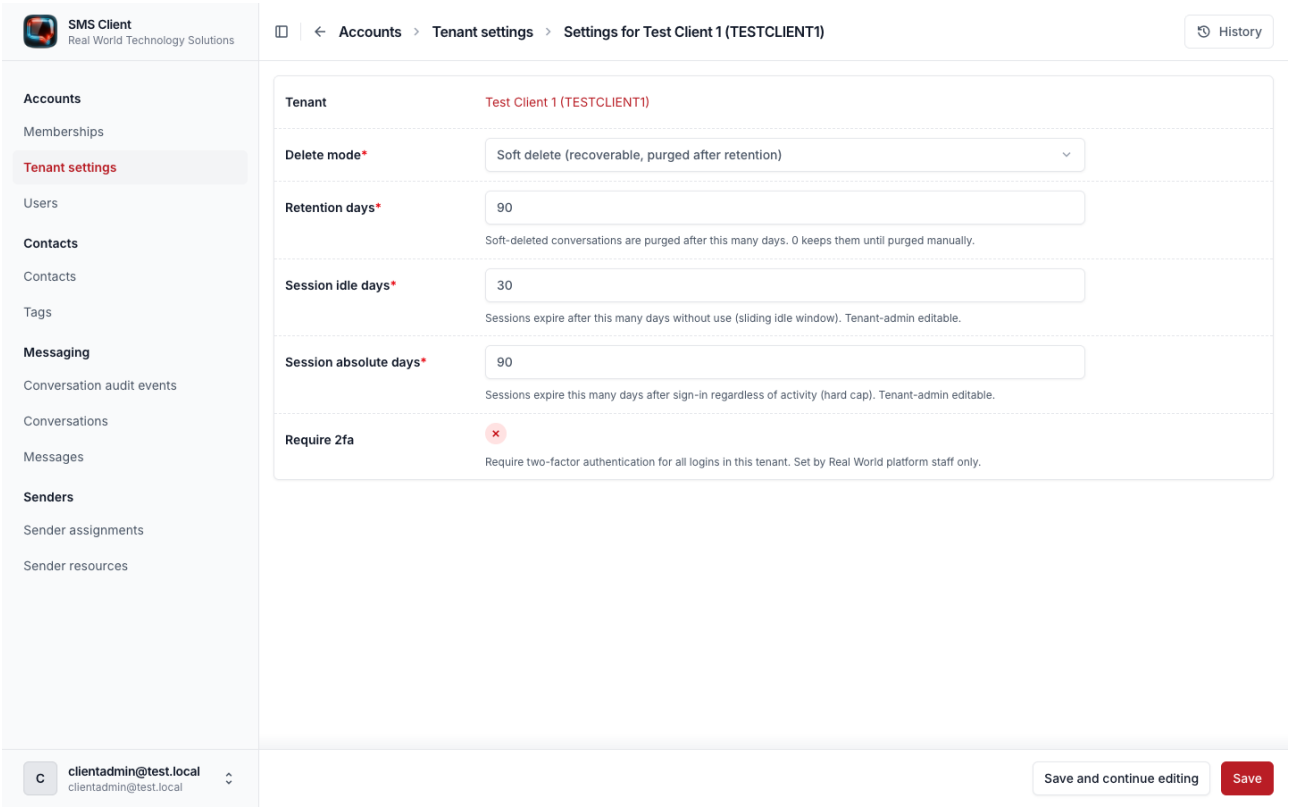

Figure 10: The Tenant settings form showing the session timeout and two-factor fields

Session timeouts

Two settings bound how long a sign-in lasts. You can edit both.

- **Session idle days** — how many days a person can go **without using** the app before they're signed out and must sign in again. The default is **30**.
- **Session absolute days** — the longest a single sign-in can last, **counting from when they signed in**, no matter how active they are. The default is **90**.

Whichever limit is reached first ends the session. Lower numbers are more secure (people sign in more often); higher numbers are more convenient. To change them, open **Tenant settings** (under **Accounts**), set the values, and click **Save**.

Requiring two-step verification

Require 2FA decides whether everyone in your organisation must use two-step verification. This setting is **managed by Real World** and shown to you as read-only — if you'd like it turned on (or off) for your organisation, contact us. When it's on, anyone who hasn't set up two-step verification is prompted to do so the next time they sign in to either the app or the administration area.

(People can always turn two-step verification on for themselves, even when it isn't required — see the user guide topic *Two-Step Verification*.)

Resetting someone's two-step verification

If a team member loses both their authenticator app and their backup codes, you can reset their two-step verification so they can set it up again.

1. Open **Users** (under **Accounts**).
2. Tick the person who needs a reset.
3. In the **Action** menu choose **Reset 2FA (delete devices + revoke sessions)** and click **Go**.

Resetting does three things at once: it removes their current two-step setup and backup codes, **signs them out everywhere** (so any lost or stolen session stops working immediately), and — if your organisation requires two-step verification — prompts them to set it up again at their next sign-in. You can only reset people **in your own organisation**, and every reset is recorded for oversight.

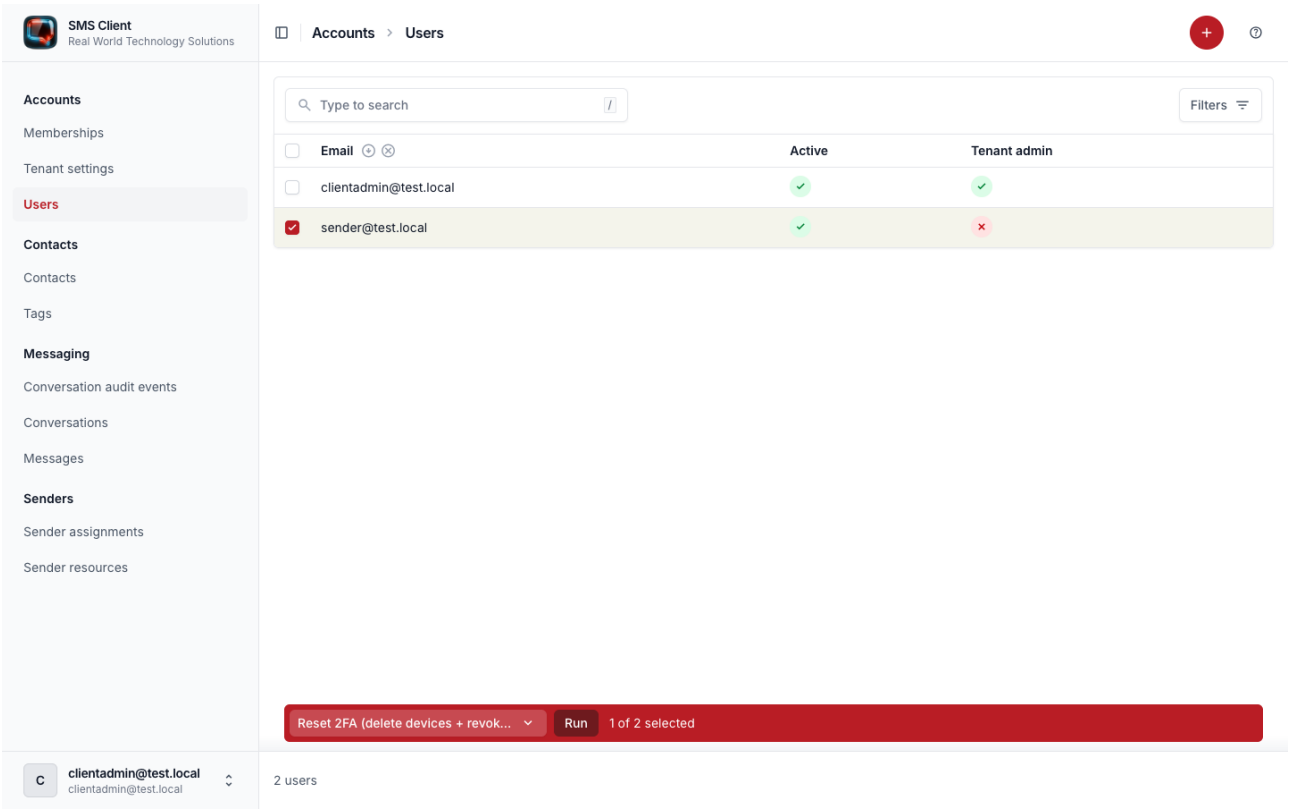

Figure 11: The Users list with a person selected and the Reset 2FA action chosen

real world technology solutions

Your Plan & Monthly Usage

Your organisation is on one of three SMS Client plans — **Essentials**, **Team**, or **Business**. The plan sets how many users you can have and which settings you can manage yourself:

	ESSENTIALS	TEAM	BUSINESS
Users included	Up to 5	Up to 20	Up to 50
Retention policy & audit trail	Managed for you	You manage it	You manage it
Organisation-wide enforced 2FA	—	Included	Included
Custom session timeout policy	—	Included	Included

On Essentials, the safe defaults still apply (soft delete with a 90-day retention window, standard session lifetimes) — you just can't change them. Settings your plan doesn't include appear locked in **Tenant settings**. To change plans, talk to Real World on **1300 798 718**.

The usage page

Administrators see a **Usage** entry in the app's top navigation. It shows, for the current calendar month (Australian Eastern time):

- **Messages sent** and **message parts sent** — long messages split into parts and each part is billed; the composer shows the part count before you send.
- **Messages received** — always free.

Monthly sending limits

Every plan includes a generous monthly sending limit to protect you from runaway or unauthorised sending. When your organisation reaches **80%** of the limit, administrators see a warning in the app; at **100%**, sending is paused until the new month starts.

A busy month is not a problem — call Real World on **1300 798 718** and we can raise the limit for your organisation.

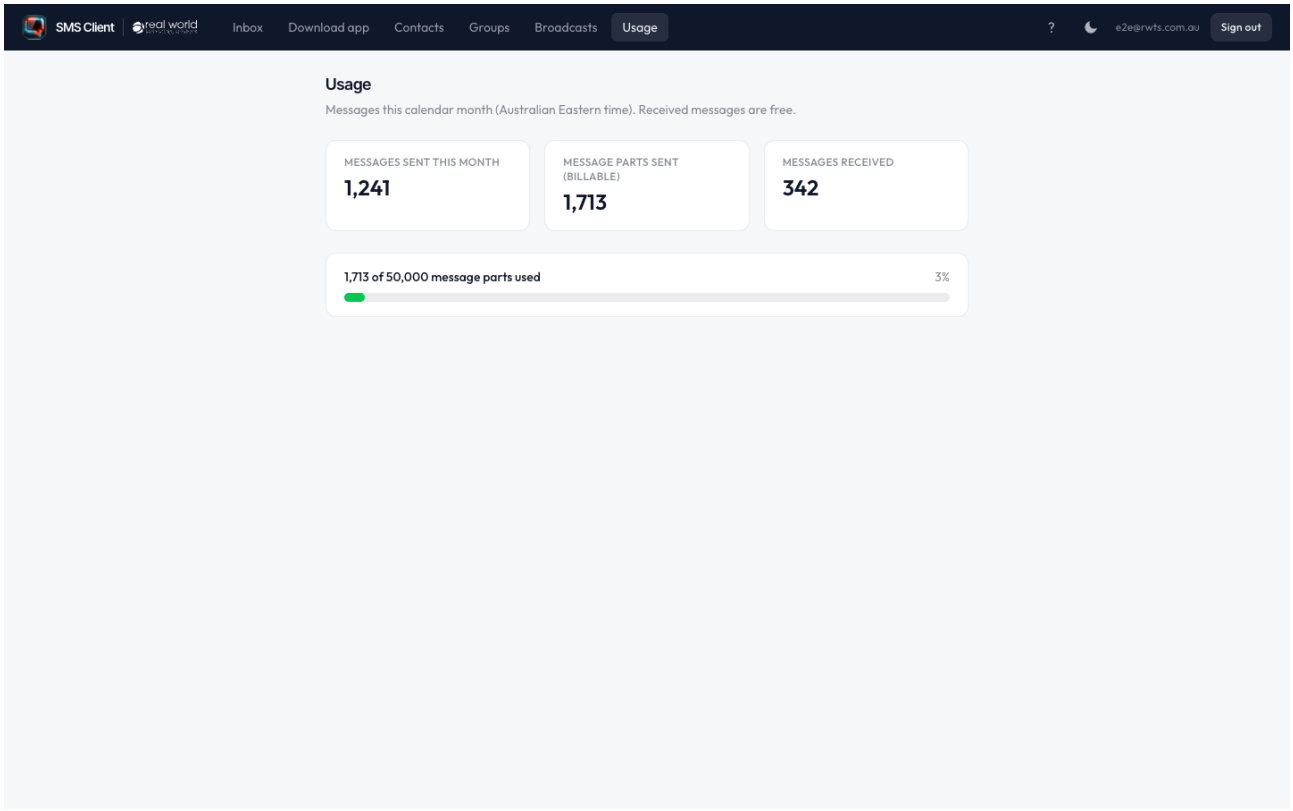

Figure 12: The Usage page showing the month's counts and the limit bar

real world technology solutions

Managing Opt-outs

An opt-out is a record that a recipient has asked not to receive marketing messages from your organisation. When someone opts out, the system suppresses them from all future marketing broadcasts so that no one on your team can accidentally send them a marketing message again.

How recipients opt out

Recipients can opt out in two ways:

- **Replying STOP** — if you use a two-way number or number pool, a recipient can reply STOP (or UNSUBSCRIBE, CANCEL, or QUIT) to any message. The system detects those keywords automatically and records the opt-out.
- **Clicking the unsubscribe link** — every marketing message sent from an alphanumeric sender ID automatically includes an unsubscribe line at the end. Clicking that link takes the recipient to a confirmation page; confirming it records the opt-out.

Marketing vs non-marketing broadcasts

When you (or a team member) creates a broadcast, the composer asks you to declare whether it is a **Marketing** or **Non-marketing** message:

- **Marketing** — the broadcast automatically includes an unsubscribe line, and anyone who has opted out is silently skipped. You will see the live recipient count drop to reflect this suppression before you send.
- **Non-marketing** — the broadcast is treated as a service communication (for example, an appointment reminder or a delivery notification). Opted-out recipients are **not** skipped, because opt-outs apply to marketing only. The composer displays a warning to remind you of this whenever opted-out numbers are in your audience. Non-marketing broadcasts can optionally carry the opt-out footer too — the sender sees a toggle in the composer that starts in the position you set for your organisation (see *Customising the opt-out footer* below).

Only mark a broadcast non-marketing when it genuinely is a service or transactional message. Sending marketing content as non-marketing is a misuse of the override and may put your organisation in breach of the Australian Spam Act (see Compliance note below).

Viewing and managing the opt-out list

Open **Opt-outs** under the **Messaging** section of the administration area. The list shows each opted-out number, the reason it was recorded (STOP reply or unsubscribe link), and the date it was added.

You can manage the list in two ways:

- **Add a number manually** — use the **Add opt-out** button to record an opt-out on behalf of a recipient who asked by some other channel (for example, by phone or email). Enter the number and save; they will be suppressed from future marketing broadcasts immediately.
- **Delete an entry to resubscribe** — if a recipient contacts you and explicitly asks to be resubscribed, tick their entry and use the **Delete selected** action. Once removed, they will receive marketing broadcasts again. Always confirm the recipient's intent before doing this.
- **Export the list** — tick the entries you need (or select all) and use the **Export selected opt-outs to CSV** action. The file contains the phone number, how the opt-out was recorded, the originating broadcast (if any), and the date it was added — useful as compliance evidence or when moving to another platform.

Customising the opt-out footer

Open **Tenant settings** under the **Accounts** section of the administration area to control how the footer behaves for your organisation:

- **Opt-out footer enabled** — whether non-marketing broadcasts include the footer by default. Senders can still switch it on or off for an individual broadcast in the composer. This setting has no effect on marketing broadcasts, which always include the footer.
- **Opt-out footer text** — the footer wording used on non-marketing broadcasts sent from reply-capable senders (two-way numbers and pools). The default is "Reply STOP to opt out". If you customise it, keep a clear STOP instruction so recipients know how to opt out.

Two notes on scope: one-way alphanumeric sender IDs always use the unsubscribe-link form of the footer (recipients cannot reply to them), so the custom wording does not apply there. Marketing broadcasts always use the standard compliance wording regardless of this setting.

Compliance note

Honouring opt-outs for marketing messages is a legal requirement under the Australian Spam Act 2003. The law requires that you action an opt-out promptly (within five business days at the most). This system records and acts on opt-outs immediately, but it is your responsibility to ensure team members do not use the non-marketing override to bypass suppression for content that is genuinely marketing material.

Real World Technology Solutions publishes two policies that govern sender identity and complaint handling for this service. Please make sure your team is familiar with both:

- SMS Sender ID Register — how sender IDs are registered and the obligations that attach to them.
- SMS Sender ID Compliance & Complaints Policy — the standards your messaging must meet and how complaints are handled.

Next steps

- Sending a Broadcast — how to choose the message type and review the suppressed recipient count before sending.

Single Sign-On: Setup, Domains & Role Mapping

Settings → Single Sign-On lets you connect your own identity provider (IdP) — such as Keycloak, Microsoft Entra ID, Google Workspace, or Duo — so your team signs in with their existing organisational login instead of a separate SMS Client password.

> **Plan note:** single sign-on is available on the **Business** plan — see *Your Plan & Monthly Usage*. If the Single Sign-On item isn't visible in Settings, your plan doesn't include it yet; contact Real World to upgrade.

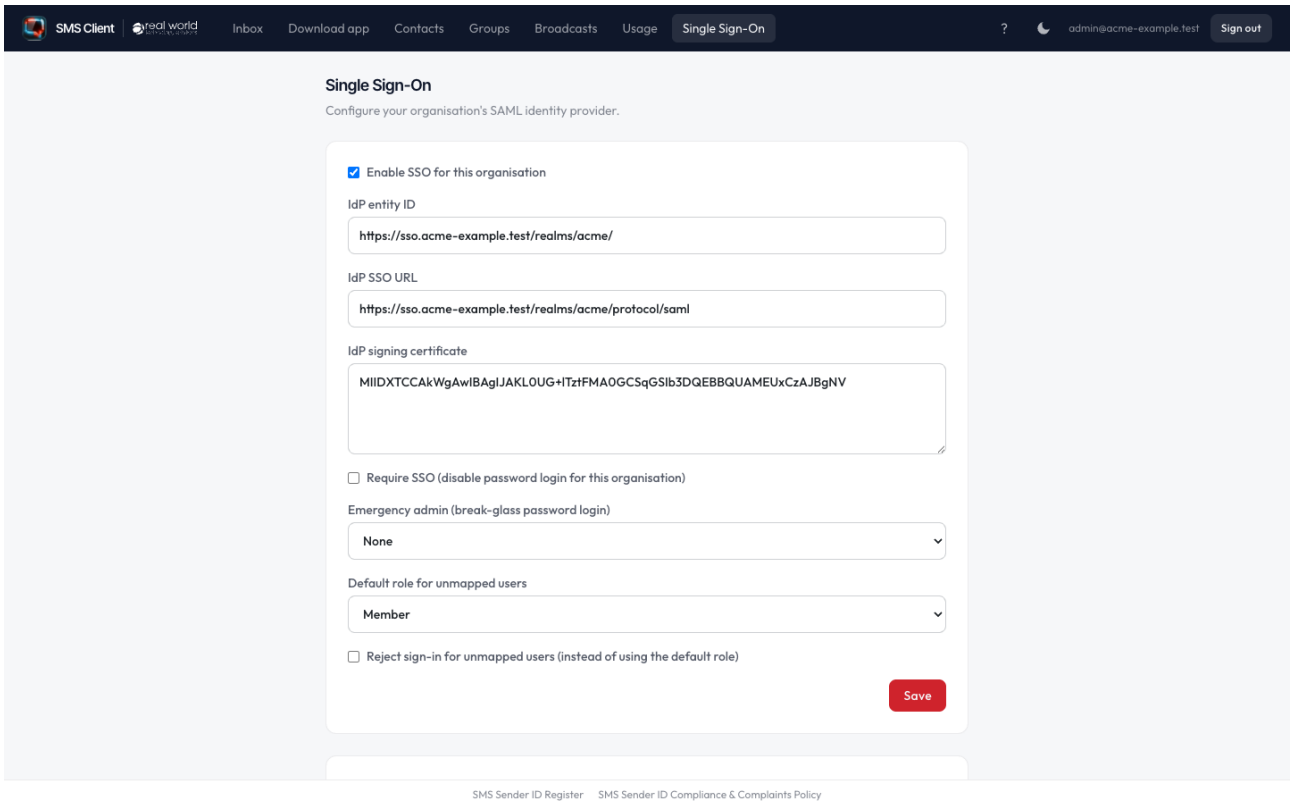

Figure 13: The Single Sign-On settings page showing the identity provider fields, the enforce-SSO toggle, the emergency admin picker, and the default-role controls

For step-by-step instructions for your specific identity provider, see *Setting Up SSO With Keycloak*, *Setting Up SSO With Microsoft Entra ID*, *Setting Up SSO With Google Workspace*, or *Setting Up SSO With Duo*.

The two-way handshake

Setting up SSO means giving two systems each other's details:

- **Your SP details** (shown on this page, under **Your SP details**) — give these to your identity provider when you register the SMS Client as an application there. **SP entity ID / metadata URL** and **ACS URL** are fixed for your organisation and won't change.
- **Your identity provider's details** — after you register the SMS Client in your IdP, it will give you back an **entity ID**, an **SSO URL**, and a **signing certificate**. Paste those into the **IdP entity ID**, **IdP SSO URL**, and **IdP signing certificate** fields on this page.

Tick **Enable SSO for this organisation** and click **Save** once both sides are filled in. Sign-in won't be offered to your team until this is on.

Verified domains

Before anyone can sign in with SSO, you need to prove your organisation owns the email domain(s) your team signs in with.

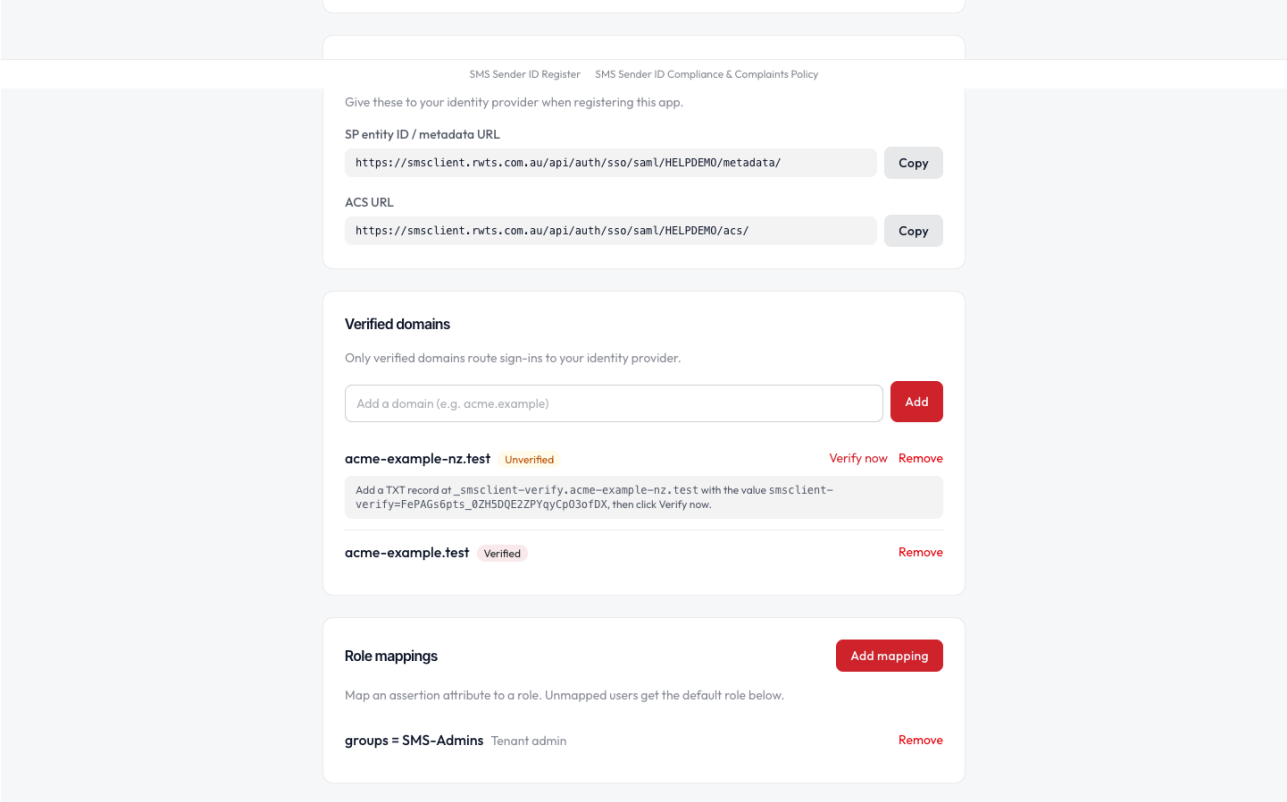

Figure 14: The verified domains list showing one verified and one unverified domain, with the DNS TXT instructions for the unverified one

1. Type your domain (e.g. `acme.example`) into **Add a domain** and click **Add**.
2. The new domain shows a DNS TXT record to add: a name starting with `_smsclient-verify.` and a value starting with `smsclient-verify=`. Add this record with whoever manages your domain's DNS.
3. Once the record is live (this can take a few minutes to propagate), click **Verify now** on that domain.

Only **verified** domains route sign-ins to your identity provider — an unverified domain is treated the same as one you haven't added at all, so nobody can accidentally be routed to the wrong organisation's login.

Role mapping

Role mapping decides what a person can do in the SMS Client based on information your identity provider sends when they sign in (an **attribute**, sometimes called a claim — commonly their group membership).

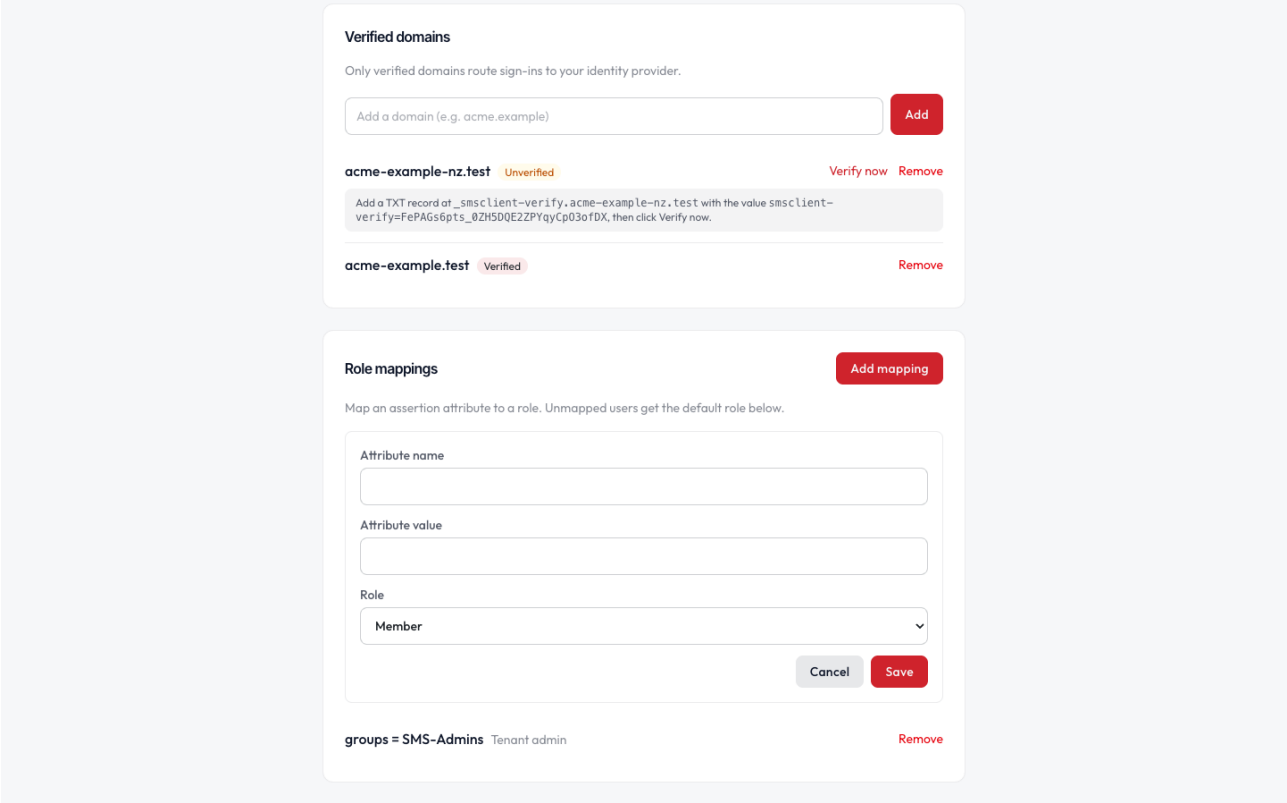

Figure 15: The role mappings list with one mapping (an attribute name/value pair mapped to a role) and the add-mapping form open

1. Click **Add mapping**.
2. Enter the **attribute name** your identity provider sends (e.g. `groups`) and the **attribute value** that should grant the role (e.g. the name of a group in your directory).
3. Choose the **role**: **Member** (regular access) or **Tenant admin** (can manage your organisation's users and settings — the same level of access as *Making Someone an Administrator* grants manually).
4. Click **Save**.

Default role for unmapped users decides what happens to someone who signs in successfully but doesn't match any mapping — they're given this role. Turn on **Reject sign-in for unmapped users** instead if you'd rather those sign-ins be refused outright than quietly become ordinary members.

Role mapping is re-evaluated **every time someone signs in** — if you remove someone from a group in your directory, they lose the matching role the next time they sign in, automatically.

Requiring SSO (and the break-glass account)

Require SSO (disable password login for this organisation) turns off password sign-in for your team entirely — everyone must use your identity provider, for both the app and (if they're an administrator) the administration area.

> **Before you turn this on:** choose an **Emergency admin** — one person in your organisation who keeps a working SMS Client password even when SSO is required, in case your identity provider ever has an outage. Without one, only Real World platform staff could get your team back in.

Pick the emergency admin from the dropdown (any member of your organisation) and click **Save**.

Sign-in history

Every SSO sign-in attempt — successful or not — is recorded for oversight, including which role was applied and why a sign-in was refused if it was. This history isn't self-service; contact Real World if you need to review it.

real world technology solutions

Setting Up SSO With Keycloak

This walks through connecting a self-hosted or managed **Keycloak** realm as your identity provider. See *Single Sign-On: Setup, Domains & Role Mapping* first for the concepts (SP details, domains, role mapping) this guide assumes.

1. Get your SP details from the SMS Client

Open **Settings → Single Sign-On** and copy the two values under **Your SP details**: the **SP entity ID / metadata URL** and the **ACS URL**. You'll need both in the next step.

2. Create a SAML client in Keycloak

1. In the Keycloak admin console, select the realm your team signs into.
2. Go to **Clients → Create client**.
3. Set **Client type** to **SAML**.
4. Set **Client ID** to the **SP entity ID / metadata URL** you copied.
5. Under **Valid redirect URIs** (or **Assertion Consumer Service URL**, depending on your Keycloak version), enter the **ACS URL** you copied.
6. Save the client.

3. Configure the SAML client's settings

In the new client's **Settings** tab:

- Turn on **Sign documents** — this signs the SAML *response*, which the SMS Client requires. **Sign assertions** is a separate toggle that signs only the assertion inside the response; leaving **Sign documents** off will cause sign-in to fail even if **Sign assertions** is on.
- Set **Name ID format** to **Email**.
- Leave **Client signature required** off unless you have a specific reason to require signed requests from the SMS Client.

4. Map a group (or role) into an attribute

Under the client's **Client scopes**, add a mapper (or edit the default one):

1. Add a mapper of type **Group list** (or **User attribute**, if you'd rather map a specific attribute instead of group membership).
2. Set the mapper's **Name** and **SAML Attribute Name** to something simple and memorable — e.g. `groups`. This is the **attribute name** you'll use in role mapping back in the SMS Client.
3. Save.

Any group name Keycloak sends through this mapper becomes an **attribute value** you can map to a role — see *Single Sign-On: Setup, Domains & Role Mapping* for how to add the mapping itself.

5. Get Keycloak's details and finish the SMS Client side

1. In Keycloak, open the realm's **Realm settings → General → Endpoints** and open the **SAML 2.0 Identity Provider Metadata** link — this page (or its underlying XML) contains the realm's **entity ID**, its **SSO endpoint URL**, and its **signing certificate**.
2. Back in **Settings → Single Sign-On** in the SMS Client, paste those three values into **IdP entity ID**, **IdP SSO URL**, and **IdP signing certificate**.
3. Tick **Enable SSO for this organisation** and click **Save**.
4. Add and verify your email domain, then add a role mapping using the attribute name you set in step 4.
5. Test by signing out and back in with an account in the mapped group.

real world technology solutions

Setting Up SSO With Microsoft Entra ID

This walks through connecting **Microsoft Entra ID** (formerly Azure Active Directory) as your identity provider. See *Single Sign-On: Setup, Domains & Role Mapping* first for the concepts this guide assumes.

1. Get your SP details from the SMS Client

Open **Settings → Single Sign-On** and copy the two values under **Your SP details**: the **SP entity ID / metadata URL** and the **ACS URL**.

2. Create an enterprise application

1. In the Microsoft Entra admin center, go to **Enterprise applications → New application → Create your own application**.
2. Give it a name (e.g. "SMS Client") and choose **Integrate any other application you don't find in the gallery**.
3. Once created, open the application and go to **Single sign-on**, then choose **SAML**.

3. Configure basic SAML settings

In **Basic SAML Configuration**, click **Edit** and set:

- **Identifier (Entity ID)** — the **SP entity ID / metadata URL** you copied.
- **Reply URL (Assertion Consumer Service URL)** — the **ACS URL** you copied.

Save. Then, under **SAML Certificates**, set **Signing Option** to **Sign SAML response** (or **Sign SAML response and assertion**). Entra ID's default, **Sign SAML assertion**, signs only the assertion — the SMS Client requires the response itself to be signed and will reject sign-ins from a client left on the default.

4. Configure attributes & claims

Still on the **Single sign-on** page, open **Attributes & Claims**:

- Under **Additional claims**, make sure the **Unique User Identifier (Name ID)** claim's source is set to the user's **email address**.
- Add a new claim (e.g. named `groups`) whose source is **Groups assigned to the application**, or a specific attribute your directory uses for role — this is the **attribute name** you'll use for role mapping back in the SMS Client.

> **Group claims note:** Entra ID sends group membership as object IDs, not group names, unless you configure the claim to emit a different format (e.g. under **Manage → Single sign-on → Attributes & claims → Groups returned in claim**, choose a format like **Group ID** or, where available, a friendly

> name). Whichever value it sends is the **attribute value** you'll use in role mapping — check what Entra actually sends before setting up your mapping.

5. Get Entra's details and finish the SMS Client side

1. On the **Single sign-on** page, under **SAML Certificates**, note the **Login URL**, the **Microsoft Entra Identifier**, and download the **Certificate (Base64)**.
2. Back in **Settings → Single Sign-On** in the SMS Client, paste the Microsoft Entra Identifier into **IdP entity ID**, the Login URL into **IdP SSO URL**, and the certificate contents into **IdP signing certificate**.
3. Tick **Enable SSO for this organisation** and click **Save**.
4. Add and verify your email domain, then add a role mapping using the attribute name and value from step 4.
5. Under **Users and groups** on the enterprise application, make sure the people (or groups) who should have access are assigned to the application — Entra ID only allows sign-in for assigned users.
6. Test by signing out and back in with an assigned account.

real world technology solutions

Setting Up SSO With Google Workspace

This walks through connecting **Google Workspace** as your identity provider, using a custom SAML app. See *Single Sign-On: Setup, Domains & Role Mapping* first for the concepts this guide assumes.

1. Get your SP details from the SMS Client

Open **Settings → Single Sign-On** and copy the two values under **Your SP details**: the **SP entity ID / metadata URL** and the **ACS URL**.

2. Add a custom SAML app

1. In the Google Admin console, go to **Apps → Web and mobile apps → Add app → Add custom SAML app**.
2. Give it a name (e.g. "SMS Client") and continue past the first screen — it shows Google's **SSO URL**, **Entity ID**, and **Certificate**. Keep this screen open (or download the certificate); you'll need all three.

3. Configure the service provider details

On the **Service provider details** screen, set:

- **ACS URL** — the **ACS URL** you copied from the SMS Client.
- **Entity ID** — the **SP entity ID / metadata URL** you copied.
- **Name ID format** — **EMAIL**.
- **Name ID** — **Basic information → Primary email**.
- **Signed response** — turn this **on**. Google Workspace signs only the assertion by default; the SMS Client requires the response itself to be signed.

4. Add attribute mapping

On the **Attribute mapping** screen, add a mapping for group membership (or another directory attribute you use for role), e.g. mapping Google's **Groups** field to an attribute named `groups`. This is the **attribute name** you'll use for role mapping back in the SMS Client — whatever group name Google sends becomes the **attribute value**.

> **Groups note:** Google Workspace doesn't send *all* of a user's groups by default in every configuration — check the attribute mapping screen's group options and confirm which groups are actually included before relying on a specific group name in your role mapping.

5. Finish the SMS Client side

1. Back in **Settings → Single Sign-On** in the SMS Client, paste Google's **Entity ID** into **IdP entity ID**, the **SSO URL** into **IdP SSO URL**, and the certificate contents into **IdP signing certificate** (from step 2).
2. Tick **Enable SSO for this organisation** and click **Save**.

3. Add and verify your email domain, then add a role mapping using the attribute name and value from step 4.
4. Back in the Google Admin console, turn the app **ON** for the organisational units or groups who should have access.
5. Test by signing out and back in with an account in an enabled unit.

real world technology solutions

Setting Up SSO With Duo

This walks through connecting **Duo Single Sign-On** as your identity provider, using a generic SAML service provider application. Duo handles your organisation's multi-factor prompt as part of sign-in, so nobody using Duo needs the SMS Client's own two-step verification. See *Single Sign-On: Setup, Domains & Role Mapping* first for the concepts this guide assumes.

1. Get your SP details from the SMS Client

Open **Settings → Single Sign-On** and copy the two values under **Your SP details**: the **SP entity ID / metadata URL** and the **ACS URL**.

2. Add a generic SAML service provider

1. In the Duo Admin Panel, go to **Applications → Protect an Application**.
2. Search for and choose **Generic Service Provider** (a "SAML" application type).
3. Under **SAML Response**, set:
   - **Entity ID** — the **SP entity ID / metadata URL** you copied.
   - **Assertion Consumer Service (ACS) URL** — the **ACS URL** you copied.
   - **NameID format** — **Email Address**, sourced from the user's email.
4. Make sure **Sign response** (or equivalent) is turned on, not just **Sign assertion** — the SMS Client requires the SAML response itself to be signed.

3. Map a group into an attribute

Under the application's attribute or mapping settings, map the user's Duo group membership (or a directory attribute) to an outgoing SAML attribute — e.g. name it `groups`. This is the **attribute name** you'll use for role mapping back in the SMS Client; the group name Duo sends is the **attribute value**.

4. Get Duo's details and finish the SMS Client side

1. On the application's configuration page, note the **Single Sign-On URL**, the **Entity ID**, and download the **Certificate**.
2. Back in **Settings → Single Sign-On** in the SMS Client, paste Duo's Entity ID into **IdP entity ID**, the Single Sign-On URL into **IdP SSO URL**, and the certificate contents into **IdP signing certificate**.
3. Tick **Enable SSO for this organisation** and click **Save**.
4. Add and verify your email domain, then add a role mapping using the attribute name and value from step 3.
5. In Duo, assign the application to the users or groups who should have access.
6. Test by signing out and back in with an assigned account — you should be prompted with Duo's own multi-factor challenge before returning to the SMS Client, already signed in.

Using Duo for Real World platform administrators

If you're setting this up as a **Real World** platform administrator (not a customer organisation), this same Duo connection is also how authorised staff can sign in to the Django administration area itself, and — for the one designated platform configuration only — be granted system administrator access based on Duo group membership. That elevation path is managed entirely by Real World platform staff and is not part of a customer organisation's self-service setup.